Public Document Pack

AUDIT COMMITTEE

Thursday, 19 July 2018 | **6.00 pm** | **Committee Room 1, City Hall**

Membership:	Councillors Geoff Ellis (Chair), Sue Burke (Vice-Chair), Thomas Dyer, Jim Hanrahan, Laura McWilliams, Gary Hewson and Ronald Hills
Independent Member:	Jane Nellist
Officers attending:	Democratic Services, Jaclyn Gibson, John Scott, Rob Baxter and Gavin Thomas

A G E N D A

SECTION A **Page(s)**

11.	Nominations - Audit Committee Forum Date: 16 October 2018 Venue: The Council Chamber, North Kesteven District Council, Kesteven Street, Sleaford. NG34 7EF Time: 9.30 – 4pm	**Verbal Report**
12.	Audit Committee Work Programme	**181 - 186**

Audit Committee **14 June 2018**

Present:	Councillor Geoff Ellis *(in the Chair)*
Councillors:	Kathleen Brothwell, Thomas Dyer, Jim Hanrahan, Gary Hewson, Ronald Hills and Laura McWilliams
Independent Member:	None.
Apologies for Absence:	Councillor Sue Burke

1. Training

Members of Audit Committee received a training session in relation to the Statement of Accounts immediately prior to the start of the meeting in order to help them take an informed view on the contents of associated agenda items.

2. Confirmation of Minutes - 27 March 2018

RESOLVED that the minutes of the meeting held on 27 March 2018 be confirmed, subject to the following amendments:

- Minute No: 49 Review of the Constitution – Financial Procedure Rules
  That the amended motion that paragraph 7.1.5 of Financial Procedure Rules remained as the status quo without any changes be recorded as proposed by Councillor Dyer and seconded by Councillor Hewson.
- A typographical error on page 8 of the minutes referring to the Council's Vision 20290 be amended to read 'Vision 2020'.

3. Matters Arising

Minute No 42: Matters Arising

Mike Norman, representing KPMG, confirmed that the Draft External Audit Account 2018/19 had been circulated to members since the last meeting, which included reference to EU PIE legislation and regulations.

Members asked whether the agreement for Jane Nellist to act as our Independent Member with knowledge on accountancy procedures was acceptable.

Mike Norman, representing KPMG advised this was a matter for Audit Committee to agree.

The Chair confirmed that there had been no challenge from members of Audit Committee to this suggestion, therefore Jane Nellist had kindly accepted this role.

4. Declarations of Interest

Councillor Jim Hanrahan declared a Personal and Pecuniary Interest with regard to the agenda item titled 'Draft Statement of Accounts 2017/18'.

Reason: As a member of the Local Government Pension Scheme. He did not leave the room as this subject matter was not mentioned during discussions held.

5. Annual Governance Statement 2017/18

Pat Jukes, Business Manager, Corporate Policy:

a. presented Audit Committee with the 2017/18 Annual Governance Statement (AGS)

b. tabled a revision to paragraph 1.3 of the AGS Statement 2017/18 under 'Key Elements of Council's Governance Framework' which included additional text in respect of Risk Management as follows:

- *The Council's arrangements comply with the requirements of the CIPFA Statement on the Role of the Head of Internal Audit (2010)*

c. stated that the updated AGS Statement 2017/18 would be re-signed off by the Leader of the Council and Chief Executive

d. reported that a senior officers group consisting of City Solicitor, Chief Finance Officer, Assistant Director Strategic Development, Finance Manager and Audit Manager had reviewed the levels of governance assurance provided for all services and projects, looking at a range of areas from Internal Audit results and identified risks to performance outturn

e. highlighted that the AGS included a range of areas the Council had completed/achieved in 2017/18 as well as some key areas it intended to pursue during 2018/19

f. referred to the key documents attached within her report at paragraph 2.4

g. summarised the changes from 2016/17 to 2017/18 as detailed at paragraph 2.5 of the report detailing several issues that had been significantly progressed and removed, and one current significant issue, namely information management which would remain a focus for 2018/19

h. advised that there were no new areas designated as significant issues

i. outlined other areas not considered significant issues yet for a focus to be retained a focus on in relation to:

- The process of setting up a new partnership company if required in order to implement correct government arrangements
- Project management monitoring arrangements
- Western Growth Corridor
- To continually ensure timely professional advice was sought on key projects, policies and decisions
- Rolling out of Responsible Officer duties within Housing Service during 2018/19

j. invited members' questions and comments.

Members requested that the document 'Key Elements of Council's Governance Framework' included reference to members ability to request call-in and reconsideration of an Executive decision outside of scrutiny and review, in addition to it already forming part of the standing orders of the Council.

RESOLVED that the 2017/18 Annual Governance Statement be noted, with a view to monitoring progress on the single issue and those designated as 'areas to watch' over the coming year subject to the following two additional text entries in the table at paragraph 1.3 Key Elements of Council's Governance Framework' as follows:

- Risk Management
  The Council's arrangements comply with the requirements of the CIPFA Statement on the Role of the Head of Internal Audit (2010)
- Call- In
  Any two members can hold the Executive to account outside of scrutiny and review by requesting Call-In and reconsideration of an Executive decision.

6. Draft Statement of Accounts 2017/18

Robert Baxter, Financial Services Manager:

a. presented the draft Statement of Accounts to the Audit Committee for the financial year ending 31 March 2018, providing a comprehensive picture of the Council's financial circumstances to demonstrate probity and stewardship of public funds, together with a short summary of the key issues reflected in the statutory financial statements for scrutiny

b. advised that the Council was statutorily required to publish its Statement of Accounts for 2017/18 with an audit opinion and certificate by 31 July 2018

c. detailed the timescales involved with the approval of the Statement of Accounts for 2017/18 as follows:

- Report draft accounts to Audit Committee 14 June 2018
- Report to Audit Committee 19 July 2018
- Report to the Executive 23 July 2018
- Approval by Council 24 July 2018

d. guided the Audit Committee through a summary of key issues in the financial statements as detailed within the officer's report

e. highlighted that the Statement of Accounts for 2017/18 were still subject to external audit, with the preliminary stages of the audit commenced in early June; any material changes as a result of the external audit work would be reported to the meeting of the Audit Committee on 19 July 2018 when the audited Statement of Accounts would be presented for approval

f. reported that the Council had to make the Statement of Accounts available for public inspection for 30 working days, which would run from 1 June 2017 to 12 July 2018 with the external auditor being available to answer questions during this period

g. invited members' questions and comments.

Members considered the content of the report in further detail, raising queries as follows:

- Would the loss of several businesses in the City affect the Business Rates Adjustment Account?

- Officer response: This account acted as an 'adjustment' account to absorb timing differences between statutory accounting requirements and full accruals accounting. Any reduction of income would be reflected accordingly in the Collection Fund Account.
- To what did the reference within the Collection Fund Statement to income from the Ministry of Defence refer?
- Officer response: It was suspected this related to Council tax on Ministry of Defence properties, although officers would seek confirmation on this matter and report back to members of Audit Committee'

RESOLVED that:

1. Confirmation of the type of income received by the authority from the Ministry of Defence as detailed within the Collection Fund Statement be provided to members.

2. The Statement of Accounts for the financial year ending 31 March 2018, subject to external audit review, be noted.

7. Annual Internal Audit Report 2017/18

John Scott, Audit Manager:

a. presented the Audit Committee with the Annual Internal Audit Report, which outlined internal audit work undertaken during 2017/18 and, in particular:

    - included an opinion on the overall adequacy of and effectiveness of the governance framework and internal control system, together with the extent to which the Council could rely on it
    - informed how the audit plan was discharged and the overall outcomes of work undertaken
    - drew attention to any issues particularly relevant to the Annual Governance Statement

b. reported that the Annual Internal Audit Report assessed the Council as substantial, which indicated that the Council was performing well with no concerns significantly affecting the governance framework and successful delivery of the Council's priorities

c. confirmed that the Annual Internal Audit Report provided an overall positive position

d. invited members' questions and comments.

RESOLVED that the Annual Internal Audit Report be noted.

8. Internal Audit Progress Report

John Scott, Audit Manager:

a. presented the Internal Audit progress report to the Audit Committee, which covered the following areas:

    - Progress against the plan
    - Summary of audit work

- Implementation of audit recommendations
- Current areas of interest relevant to Audit Committee

b. advised that the 2017/18 Audit Plan was virtually complete, with final reports issued in relation to:

- Vision 2020 (Substantial Assurance)
- Procurement (Substantial Assurance)
- Licensing of Houses in Multiple Occupation (Limited Assurance)

c. highlighted two other audits nearing completion in respect of Planned Maintenance and Council Tax

d. outlined the current 2018/19 Audit Plan schedule as detailed at Appendix 2 to his report

e. provided performance details of planned work for the 2018/19 audit at Appendix 4 to the report

f. presented an overview of medium and high priority recommendations overdue and not yet due, as at 15 March 2018 at paragraph 8 and Appendix 5 of the report

g. invited members' questions and comments.

Simon Colburn, Assistant Director, Health and Environmental Services, updated Audit Committee on progress with the Licensing of Houses in Multiple Occupation, which received limited assurance from its recent Audit as follows:

- Officers were taking action to 'shore up' the weak areas identified by the audit.
- The service area had been aware of many of these issues and the audit had helped to shape our future work programme.
- He had requested that the area be re-audited in December 2018 to ensure all outstanding issues had been completed.
- Licensing of Houses in Multiple Occupation was an important part of the service areas work. Of the last 130 licences issued, no properties had been identified as having Category 1 hazards.
- He was confident that there were no licensed properties that were unsafe or properties remaining unlicensed in error.
- An action plan was in place to address the issues identified.
- A further update would be provided to Audit Committee in December 2018 following re-audit of the HMO service area.

Members discussed the content of the report in further detail, raising queries as follows:

- When a property adopted flexible use between a HMO/private house, how was this monitored on Council records?
- Officer response: All HMO's must comply with relevant legislation. The database was shared with other officers within the authority including the Planning Section who were alerted of any changes. He would formally collaborate with the Head of Planning to ensure this particular matter was monitored.

- How would the new HMO legislation coming into effect on 1 October 2018, which required registration of properties less than three storey in height impact on the council's workload?
- Officer response: The new regulations would require the same level of scrutiny. An additional post would be recruited to carry out inspections, subject to Executive approval.
- Did the Council liaise with the housing office at the University of Lincoln?
- Officer response: Yes, an ongoing working group included representatives from the University. A mechanism was also in place to share any complaints raised by students.
- Arrangements put in place to deal with the new HMO legislation should be considered by Policy Scrutiny Committee in October 2018. Would concerns such as the need to provide gas certificates be covered within the adoption of a revised enforcement policy to reflect the new legislation? This would be need to be considered by Performance Scrutiny Committee once the policy had time to become embedded.
- Officer response: Action to update the enforcement policy was included within the relevant service area's work programme. A signed off statement would be presented to Policy Scrutiny Committee confirming the new standards/legislation for HMO's and that information and intelligence received was shared with the Planning Manager. Automatic reminders would be generated to ensure copies of gas certificates were forwarded to the council by landlords. Meanwhile, the authority had the power to enforce HMO conditions under primary legislation and was able to prosecute offenders or serve prohibition notices as and when required.
- Should elected members approach officers with HMO concerns were they entitled to relevant information on any properties not registered?
- Officer response: It was difficult to confirm this due to GDPR legislation, however, feedback would be given to complainants.
- The target dates for Boultham Park Refurbishment Programme and Western Growth Corridor had been extended again. When would these actions be finalised?
- Officer response: Completion of the revised Boultham Park Refurbishment Programme Partnership Agreement had been extended a further three months to allow work to be finalised with the Legal Team. Review of the Health and Safety Plan for the Transport Hub was pending subject to work on the top floor of the new Central Car Park still being finalised. A further update would be provided to members of Audit Committee at the next meeting to be held on 19 July 2018

RESOLVED that

1. The request for the Assistant Director, Health and Environmental Services to formally collaborate with the Head of Planning to ensure properties having adopted flexible use between a HMO/private house be monitored on Council records be actioned.

2. A further update be provided to Audit Committee in December 2018 following the re-audit of the HMO service area.

3. A further update be provided to Audit Committee on 19 July 2018 in respect of target dates set for Boultham Park Refurbishment Programme Partnership Agreement and the Health and Safety Plan for the Transport Hub.

4. The contents of the report be noted and further monitoring arrangements be continued.

9. Fraud and Error Update Report (2017/18) 12 Months

John Scott, Audit Manager:

a. presented his report on counter fraud arrangements 2017/18 for members' consideration, which covered the following main areas:

- An update on the Lincolnshire Counter Fraud Partnership (LCFP)
- A position statement on the National Fraud Initiative.
- Fraud work within housing benefits and other areas.
- An update on counter fraud outcomes

b. updated members on the key messages in relation to the LCFP, areas of progress in 2017/18, and key areas and themes for 2018/19 as highlighted within paragraph 3 of his report

c. highlighted City of Lincoln Council activity in relation to counter fraud arrangements at paragraph 4 of the report

d. requested member's comments on the content of the report.

Jane Nellist, Independent Member, highlighted that insurance values/claims fluctuated year on year together with notices served to quit in relation to housing sub-letting and asked whether any investigations had been made as to the reason for this?

John Scott, Audit Manager advised that he would check back through housing data over the last 3 years and seek comments from Housing officers to report back to Audit Committee at the next meeting.

RESOLVED that:

1. Any trends over the past 3-4 years in terms of insurance values/claims/notices served to quit be reported back to members of Audit Committee on 19 July 2018.

2. The content of the report be noted and monitoring arrangements be continued.

10. Audit Committee Work Programme 2018/19

John Scott, Audit Manager:

a. presented the Audit Committee with its 2018/19 work programme

b. invited members' questions and comments.

RESOLVED that the 2018/19 work programme be noted, subject to the following additions to the items to be considered at the 19 July 2018 meeting:

- Update on new External Auditors
- Update on Housing Benefit Fraud Policy

- Update: Target dates set for Boultham Park Refurbishment Programme Partnership Agreement and the Health and Safety Plan for the Transport Hub.

AUDIT COMMITTEE **19 JULY 2018**

SUBJECT:	**INFORMATION MANAGEMENT POLICIES**
DIRECTORATE:	**CHIEF EXECUTIVE & TOWN CLERK**
REPORT AUTHOR:	**DATA PROTECTION OFFICER & LEGAL & DEMOCRATIC SERVICES MANAGER**

1. Purpose of Report

1.1 To seek approval of the Information Management Policies required in accordance with the EU General Data Protection Regulation and the Data Protection Act 2018.

2. Executive Summary

2.1 Data protection is critical to the Council to ensure that the data which is received, processed, retained and shared is protected in accordance with the legal framework.

2.2 The Data Protection Act 1988 has been replaced by a new Data Protection Act 2018 (DPA). The Information Commissioners' Office (ICO) state that;

'*The new DPA aims to modernise data protection laws and to ensure they are effective in the years to come'.*

The EU General Data Protection Regulation (GDPR) became directly applicable from the 25th May 2018, although the new DPA supplements the GDPR and both need to be read side by side.

2.3 The Council needs to have policies to enable the Council to be compliant with the new legal framework and the information governance team need to roll out the policies in order to increase awareness of the GDPR to officers' and councillors. Therefore members of the public can be confident that the organisation are aware of their responsibilities of the new legal framework.

3. Background

3.1 Many of the DPA and the GDPR's main concepts and principles are much the same as those in the previous Data Protection Act. However, there are new elements, which include increased access rights for individuals, to include developments in new technology, tighter time limits for reporting breaches and increased fines for breaching data protection legislation and associated powers of the Information Commissioner's Officer.

3.2 Therefore as part of the action plan for this Vision 2020 project and to ensure the Council is ready for the implementation of the new Regulation, the Council needs to ensure all its policies are in place.

3.3 The information governance team prepared the General Data Protection Regulation & Data Protection Policy which went to Executive in March so that it would be in place from 25th May. This policy has been distributed to all staff through the Netconsent system which required them to review the policy by 25th May to ensure they were all aware of it. The Policy went to Policy Scrutiny Committee due to timings, however the preference is that these policies come through this Committee given its role in respect of data protection issues, as outlined in the terms of reference.

3.4 A summary sheet in relation to the GDPR and DPA has also been prepared for staff and uploaded into Netconsent for all to access.

3.5 The Information Management Policies are attached for consideration and are as follows:-

Appendix A The General Data Protection Regulation and Data Protection Policy
Appendix B The General Data Protection and Data Protection Policy Summary Sheet
Appendix C Information Governance Policy
Appendix D Legal Responsibilities Policy
Appendix E Information Sharing Policy
Appendix F Data Quality Policy
Appendix G Data Protection Breach Management Policy
Appendix H Freedom of Information Policy & Environmental Information Regulations Policy
Appendix I Records Management Policy
Appendix J Retention and Disposal Policy

4 The Data Protection Principles

4.1 The GDPR states that anyone processing personal data must apply the six data protection principles. These principles are legally enforceable. These are broadly similar to the previous Data Protection Act.

1. ***Lawfulness, fairness and transparency principle*:**

   Processed fairly, lawfully and in a transparent manner in relation to individuals;

Lawfully requires in particular that personal data not be processed unless at least one lawful basis has been met. For sensitive 'special category data' this also requires at least one further condition to be met, in addition to the lawful basis.

2. ***Purpose limitation principle:***

   Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those processes;

Further processes for archiving purposes in the public interest, scientific or historical research or statistical purposes is not considered to be incompatible with the initial purpose.

3. ***Data minimisation principle:***

   Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. ***Accuracy principle :***

   Accurate and where necessary kept up to date;

Every step must be taken to ensure personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. ***Storage limitation principle:***

   Kept in a form which permits identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed;

Personal data may only be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes. This is subject to technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. ***Integrity and confidentiality principle:***

   Processed in a manner the ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

The GDPR also introduces a further ***Accountability Principle*** which requires the Council as Controller be responsible for, and be able to demonstrate, compliance with the above principles.

4.2 The proposed policies address the above changes and any comments received from Audit committee will be referred to Executive on 23 July 2018 for their consideration.

5 Strategic Priorities

5.1 These policies do not directly relate to one of the main strategic priorities, however it does assist to make the Council fit for purpose and the intention is to publish these information governance Polices on the website to continue to promote transparency.

6. Organisational Impacts

6.1 Finance

No implications arising from this report.

6.2 Legal Implications

As outlined in the report.

6.3 Equality Diversity & Human Rights

There are no specific impacts in respect of these in this report and therefore a Equality Impact Assessment has not been carried out.

7. Risk Implications

7.1 The Council must implement policies in order to comply with the GDPR and the new Data Protection Act 2018.

8. Recommendation

8.1 To consider and approve the attached policies.

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	10
List of Background Papers:	None
Lead Officer:	Sally Brooks, Data Protection Officer Telephone (01522) 873765

The General Data Protection Regulation & Data Protection Policy

Document control

Organisation	**City of Lincoln Council**
Title	**Data Protection Policy**
Author - name and title	**Becky Scott, Legal and Democratic Services Manager**
Owner - name and title	**Becky Scott, Legal and Democratic Services Manager**
Date	**May 2018**
Approvals	**March 2018 - Executive**
Filename	**Data Protection Policy**
Version	**V.2.0**
Next review date	**May 2020**

Document Amendment history

Revision	Originator of change	Date of change	Change description
V.2.0	**Data Protection Officer**	**May 2018**	**To incorporate GDPR and Data Protection Bill- following Royal Assent to be DPA 2018.**

Contents

Overview

To perform efficiently the City of Lincoln Council ("the council"), must collect and use information about the individuals with whom we work. This may include members of the public, employees (past and prospective), volunteers, work experience, partner organisations, agents, customers, and suppliers. The council may also be required by law to collect and use information to meet the requirements of central government.

All personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means. We all have a responsibility for its safe handling.

This document sets out the principles of data protection; our responsibilities; the rights of individuals; information sharing; and how we shall deal with complaints. The council must comply and fully endorses the principles of data protection as set out in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

The council is a data Controller and is therefore bound by a legal duty to meet its obligations under the GDPR and the DPA at all times, when handling personal information. These legal obligations last from the moment the information is obtained until it is returned, deleted or destroyed.

1. Purpose

The main purpose of this Policy is to raise awareness amongst staff of GDPR and the DPA. This is to ensure that the council complies with its legal obligations at all times when handling personal information. The council also regards the lawful and correct treatment of personal information as essential to the effectiveness and success of its operations and in maintaining trust between the council and those with whom it carries out business. To this end the council will process personal information lawfully and correctly by embedding this Policy into its culture, its processes and its procedures.

2. Scope

2.1 Who does this Policy apply to?

This Policy applies to all full time and part time employees of the City of Lincoln Council, elected members, partner agencies, contracted employees, third party contracts (including agency employees), volunteers and students or trainees on placement with the council.

Elected members are also data Controllers in their own right and must ensure that any personal information they hold/use in their office as an elected member is treated in line with the GDPR and the DPA.

2.2 What is personal data?

This Policy applies to Personal data which means;

'any information relating to an identified or identifiable natural person ('the Data Subject'). An identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier'

The GDPR has expanded the definition of personal data to reflect changes in technology and includes online identifiers such as an IP address and location data where they directly or indirectly identify individuals. Data which has been Pseudonymised (key coded) can also fall within the definition of personal data depending on how difficult it is to attribute the pseudonym to a particular individual.

2.3 What is special category or sensitive personal data?

There are also special categories of personal data previously referred to as sensitive data which require extra protection. These are personal data revealing;

- racial or ethnic origin (for example CCTV images of individuals attending a place of worship or arrangements to allow a staff member to pray)
- political opinions
- religious or philosophical beliefs (for example veganism or atheist)
- trade union membership
- genetic or biometric data (for example fingerprints, DNA, iris and voice recognition)
- data concerning mental or physical health (for example sickness records, occupational health reports)
- sex life
- sexual orientation (including transgender and gender reassignment)
- criminal convictions and offences data are not included as special category data although similar provisions for processing apply
- all other criminal prosecutions data including investigations is dealt with separately under the Law Enforcement Provisions in the DPA and could be said to be 'extra special data'.

2.4 What type of personal records does this Policy apply to?

This Policy applies to all personal information created or held by the council, in whatever format (for example paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, Intranet, filing structure, email, filing cabinet, shelving and personal filing drawers).

The GDPR has expanded the scope of applicable information to include;

'*the processing of personal data both automated and manual which form part of a filing system, or are attending to form part of a filing system'*.

This is where personal data is accessible according to specific criteria (for example this now includes chronologically ordered sets of manual records containing personal data).

The GDPR and the DPA do not apply to information about deceased individuals, although the council may owe a duty of confidentiality in relation to such information. The GDPR and the DPA do not apply to use of personal data purely for personal or household activities.

3. Policy

3.1. The Data Protection Principles

The GDPR states that anyone processing personal data must apply the six data protection principles. These principles are legally enforceable. In summary, the principles require that personal information be:

1. **Processed fairly, lawfully and in a transparent manner in relation to individuals;**

(Lawfulness, fairness and transparency principle)

Lawfully requires in particular that personal data not be processed unless at least one Lawful Bases has been met. For special category data this also requires at least one further Condition to be met, in addition to the Lawful Basis. See the Definitions section below for a list of the Lawful Bases and additional Conditions for processing special category data.

2. **Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those processes;**

(Purpose limitation principle)

Further processes for archiving purposes in the public interest, scientific or historical research or statistical purposes is not considered to be incompatible with the initial purpose.

3. **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;**

(Data minimisation principle)

4. **Accurate and where necessary kept up to date;**

(Accuracy principle)

Every step must be taken to ensure personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. **Kept in a form which permits identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed;**

(Storage limitation principle)

Personal data may only be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes subject to technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. **Processed in a manner the ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;**

(Integrity and confidentiality principle)

The GDPR also introduces a further ***Accountability Principle*** which requires the council as Controller be responsible for, and be able to demonstrate, compliance with the above principles. This includes the council keeping records of all processing of personal data. These records are kept in the council's Information Asset Register and each IAO is responsible for keeping their section of this up-to-date and informing the Data Protection Officer of any amendments or additions. For further information please refer to the GDPR/IAO Handbook on the council's intranet here. These records of processing also include the retention and disposal schedules for each area, also available on the data protection page of the council's intranet.

3.2. Responsibilities

The City of Lincoln Council is a data Controller under the GDPR and DPA, as referred to above.

The Chief Executive has overall responsibility for ensuring compliance with the GDPR and the DPA within the council.

Directors, Assistant Directors, City Solicitor and s151 Officer (Finance) are responsible for ensuring compliance with the GDPR and DPA and this Policy within their directorates.

Information Asset Owners (IAO's) are responsible for ensuring that the business areas they have responsibility for have processes and procedures in place that comply with the GDPR and DPA and this Policy.

IT Services are responsible for ensuring that data within systems under the control of the council, cannot be accessed by unauthorised personnel and to ensure that data cannot be tampered with, lost or damaged.

Responsibility for compliance with this Policy and communicating the Policy to staff in their own business areas is delegated to the IAO's. IAO's have been advised of their responsibilities and the requirement to carry out ongoing risk assessments on the assets for which they are responsible.

The responsibility for providing day-to-day advice and guidance to support the council in complying with the GDPR and the DPA and this Policy rests with the SIRO and Data Protection Officer.

All members of staff or agency staff and elected members who hold or collect personal data are responsible for their own compliance with the GDPR and DPA and must make sure that personal information is kept and processed in-line with the GDPR, the DPA and the Staff Code of Conduct.

IAO's have responsibility for agency staff's, volunteers, work experience's compliance with the GDPR, the DPA and the Staff Code of Conduct. This includes the provision of appropriate training and inductions. IAO's must also ensure that their data protection responsibilities are communicated and handed over clearly to any successors to their IAO role.

Failure to comply for any staff member may result in disciplinary action that may lead to dismissal, in addition to the possibility of an individual being criminally prosecuted under the GDPR and the DPA and/or liable to pay compensation in any civil action.

3.3. Engaging a data Processor to process personal data on behalf of the council

If a contractor, partner organisation or agent of the council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, the lead council officer must ensure a binding contract is in place which meets the requirements of the GDPR. There is guidance on what needs to be included in these contracts in the GDPR/ IAO's Handbook available on City People here and standard clauses issued by the Crown Commercial Service available here.

If the council are Joint Controllers or Controllers in Common with a partner organisation or agent then they shall, in a transparent manner, determine their responsibilities under the GDPR and the DPA informing Data Subjects of this where applicable. Information Sharing Agreements (ISA's) may be required and these should be agreed and signed off before any work commences. The council promotes information sharing and partnership working where it is in the best interests of the Data Subject. The council has a data sharing policy and protocols in place and will keep to the standards set out in these protocols. The council as Controller must ensure, when personal data is shared, it is done in accordance with the GDPR and the DPA.

3.4 Sharing personal data with other Controllers

If the council is sharing personal data with Joint Controllers, Controllers in Common or other Controllers such as a partner organisation, agent or other council then they must do so in a transparent manner. This includes determining responsibilities under the GDPR and the DPA and informing Data Subjects of this (in privacy notices).

Information Sharing Agreements (ISA's) may be required between Controllers and these should be agreed and signed off before any work/sharing commences. These agreements should include recording the purpose of the sharing, the lawful basis, accuracy of the data, retention of data, amount of data necessary, security of the transfer, responsibility for providing privacy notices and responding to information rights requests, any duty of confidentiality owed, security of the data, single point of contact details and review dates.

The council promotes information sharing and partnership working where it is in the best interests of the Data Subject. The council has an Information Sharing Policy and protocols in place and will keep to the standards set out in these protocols. The council as a Controller must ensure, when personal data is shared, it is done in accordance with the GDPR and the DPA.

4. Rights of individuals and information access requests

The GDPR creates new rights for individuals and strengthens some of the rights that previously existed. The GDPR provides the following rights for individuals in relation to their personal data;

1. The right to be informed
2. The right to access

3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights related to automated decision making and Profiling

4.1 Right to be informed

An individual has a right to be informed of certain information concerning how their personal data will be processed. This is usually provided in a privacy notice. When and what information is supplied to the data subject depends on whether the personal data has been provided directly to the council by them or via a third party. If provided directly to the council this information must be supplied to the data subject at the time their personal data is obtained. The information must be concise, transparent, intelligible and easily accessible, as well as written in clear plain language and free of charge.

This right does not apply when the data subject already has the information and in other limited circumstances set out by the GDPR where the personal data was supplied via a third party. The Information Commissioner's Office has produced guidance in the form of a table, which summarises the information to be supplied and which is reproduced at **Appendix 1**.

4.2 The right to access

Individuals have the right to obtain confirmation their personal data is being processed, access to their data and certain information that corresponds with the information to be supplied in a privacy notice. The council must provide free of charge a copy of any data held about them and is no longer able to charge a fee for a request. However a reasonable fee can be charged when the request is manifestly unfounded or excessive, particularly if repetitive. The council may also charge a fee to provide further copies of the same information. The fee must be based on the administrative cost alone of providing the information.

Where a request is manifestly unfounded or excessive particularly repetitive the council can;

- charge a reasonable fee for the administration costs of providing the information or
- refuse the request

In refusing the request the council must explain why their request has been refused and inform them of their right to complain to the Information Commissioner's Office and to a judicial remedy without delay and at the latest within one month of the request.

The council has a right of access process, which sets out procedures for access to personal data, and complies with the GDPR and the DPA. The individual must provide proof of their identity and information may be withheld where the council is not satisfied that the person asking for information about themselves is who they say they are. In these cases, the council may refuse to provide the information until it receives all relevant requested documents.

The council must comply with the request within one month of receipt. This period can be extended by a further two months in limited circumstances where the request is complex or

numerous. In this case the council would need to inform the requester of the extension within one month of the receipt of the request and explain why the extension was necessary.

The request does not necessarily need to be made in writing under the GDPR although the council encourages requesters to utilise the council's right to access request form. If the request is made electronically the council should provide this in a commonly used electronic format.

The GDPR states that where possible the council should be able to provide remote access to secure self-service system to provide individuals with direct access to their personal data (for example the council's MyInfo system for council tax and benefits)

Where the request is for a large amount of data the GDPR allows the council to ask the individual to specify the information the request relates to.

4.3 The right to rectification

Individuals have a right to have personal data rectified if inaccurate or incomplete including by the provision of a supplementary statement. If the council has disclosed the personal data to any third parties they must inform them of the rectification where possible. The council must also inform the individual about the third parties with whom the council has disclosed the information.

The council must respond to the request for rectification within one month. As above this can be extended a further two months where the request is complex. If the council will not be taking any action to the request for rectification the requester would need to be informed of this and the reason for this explained by the council along with the individual's right to complain to the ICO and to a judicial remedy.

4.4 The right to erasure

This is not an absolute right and only applies in certain circumstances;

- where the personal data is no longer required for its purpose (kept beyond its retention period)
- where the individual withdraws their consent and this is the only legal basis for processing
- where the individual exercises their right to object to the processing and this is successful
- the personal data is being processed unlawfully (in breach of the GDPR and DPA)
- the personal data is erased to comply with a legal obligation
- the personal data relates to that of a child and is processed online with parental consent

The council may also refuse to respond to a request for erasure where personal data is processed for the following reasons;

- to exercise the right to freedom of expression and information (only likely to be relevant to press releases made by the council)
- to comply with a legal obligation or for the performance of a task carried out in the public interest or exercise of official authority (the council exercising its powers and duties provided the information held is still within its retention period)
- for public health purposes in the public interest

- archiving purposes in the public interest, scientific research or statistical purposes or
- the exercise or defence of legal claims

There are additional requirements when the request relates to children's personal data particularly online services, where they may not have been aware of the risks when they consented to the processing. This reflects the GDPR's emphasis on enhanced protection of children's personal data.

The council would also be required to inform third parties of the erasure, if they have disclosed the personal data to them, unless it is impossible or involves disproportionate effort.

4.5 The right to restrict processing

If processing is restricting following a request. The council can hold the data but not further process it. Just enough information should be retained to ensure the restriction is respected in the future.

The council would be required to comply with a request for restriction in the following circumstances;

- where the accuracy of the personal data is contested by the requester, the council would need to be able to restrict the processing until the accuracy has been verified
- where the individual has exercised their right to object to the processing (see below) and the council are considering whether its legitimate interests override those of the individual
- when the processing is unlawful and the requester opposes erasure and requests restriction instead
- where the council no longer requires the data but the individual requires this to establish, exercise or defend a legal claim.

If the council has disclosed the personal data to third parties they must inform them about the restriction unless it is impossible or involves disproportionate effort. The council must inform the individual if they decide to lift the restriction on processing at any time.

4.6 The right to data portability

This allows individual's to request transfer of their personal data from one IT environment to another in a safe and secure way without affecting its usability.

This right only applies;

- to personal data an individual has provided to the council (includes data observed from a use of a service or device)
- where the processing is based on the individual's consent or for the performance of a contract and
- when the processing is carried out by automated means

This right does not apply when the council are processing based on the Legal Basis of performance of a task in the public interest or for official functions (the council exercising its powers and duties).

The information must be provided in a structured commonly used and machine readable form (open source file such as a CSV not PDF). This must be provided free of charge within one month as other right to access requests. The same rules regarding extensions apply. If the individual requests it the council may be required to transmit the data directly to another organisation, although only where this is technically feasible.

4.7 The right to object

Individuals have a right to object when

- processing is based on legitimate interest or the performance of a task in the public interest or exercise of any official authority (for example the council exercising its powers and duties)
- direct marketing- any marketing including promoting the aims of an organisation directed to individuals
- processing for the purposes of scientific/historical research and statistics

The council would need to stop processing the personal data unless;

- it could demonstrate compelling legitimate grounds for processing which override the interest, rights and freedoms of the individual
- the processing is for the establishment, exercise or defence of legal claims
- the scientific/historical research use, unless in the public interest

The council need to inform where applicable individuals of their right to object at the first point of communication for example in the privacy notice, when obtaining their personal data.

The council must stop processing data for direct marketing as soon as they receive an objection. There are no exemptions or grounds to refuse an objection to direct marketing.

4.8 Rights related to automated decision making and profiling

Individuals have the right not to be subject to a decision when;

- it is based on automated processing and
- it produces a legal effect or a similarly significant effect on the individual

The council must ensure individuals are able to

- obtain human intervention
- express their point of view and
- obtain an explanation of the decision and challenge it

The right does not apply if the automated decision;

- is necessary for entering into a contract
- is authorised by law with safeguards in place, for example for the purposes of fraud or tax evasion or
- is based on the explicit consent of the individual which has been obtained prior to the automated processing or
- where the decision does not have a legal or similarly significant effect on an individual

If carrying out Profiling (see Definitions section below) then the council would have to ensure appropriate safeguards are in place.

- ensure processing is fair and transparent, for example provide details of the logic involved, significance and consequences (in privacy notice)
- implement technical and organisational measure to ensure inaccuracies are corrected and minimise risks of error, for example data quality checks and reviews
- keep personal data secure which is proportionate to the risk to the rights and interests of the individual and prevent discriminatory effects.

Automated decisions must not concern a child or be based on special categories of personal data unless;

- explicit consent is obtained from the individual or
- processing is necessary for reason of substantial public interest on the basis of a legal obligation with specific measures in place to safeguard the individual.

4.9. Exemptions to individual's information rights

Under the GDPR and the DPA, it is sometimes necessary to withhold certain information that has been requested by individuals in relation to the right to access. The Data Protection Officer or the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services team can offer advice in these circumstances. Examples of exemptions to right to access personal data which may be available are listed in the Definitions section below.

5. Disclosure of personal information about third parties

Personal data must not be disclosed about a third party except in line with the GDPR and the DPA. If it appears necessary to disclose information about a third party to a person requesting their personal data, advice must be sought from the Data Protection Officer or Freedom of Information Officer/the Legal and Democratic Services Manager and, if both are unavailable, a member of the legal team. Examples of exemptions to disclosure of third party personal data which may be available are listed in the Definitions section below.

6. Consent

The GDPR states that where the council are relying on the Lawful Basis to process personal data of the individual's Consent alone this must be valid. Valid Consent must be;

- unambiguous (clearly given)
- freely given (a genuine choice)
- demonstrable (the council are able to evidence the consent including when it was given)
- specific (not bundled up in the small print)
- informed (provided after being given all the information as to how the personal data will be processed, in the Privacy Notice, *see right to be informed below*)
- explicit for special categories (in writing)
- no silence or inaction (the council should not use opt-out boxes)

The individual must make a statement or a clear affirmative action to give valid Consent, for example ticking a box, entering information or clicking on an icon.

If Consent is being obtained from a child through online services and the child is under 13 years old, then parental consent is required.

Consent should rarely be relied upon as a Legal Basis for processing by the council. This is due to the issue as to whether this would be freely given, as there is a clear imbalance of power between the individual and the council. All other Legal Bases should be considered first.

7. Privacy by design and Data Protection Impact Assessments (DPIA's)

'Privacy by design' is a legal requirement for the council under the GDPR. In summary this means implementing safeguards to ensure the protection of personal data by default and from the outset of all projects. Safeguards such as technical and organisational security measures including Pseudonymisation of data and data minimisation. This requires data protection by design to be the council's default position in relation to;

- decision making
- policy formulation
- project management and
- procurement

DPIA's are the most effective way for the council to comply with our data protection obligations and to meet individual's expectations of privacy. DPIA's identify and minimise privacy risks at an early stage, reducing costs, officer time, and enforcement action by the ICO including monetary fines, legal action and damage to the council's reputation. DPIA's need imbedding in project development, to ensure the council is dynamic, competitive and able to demonstrate to 'privacy by design'.

DPIA's particularly screening assessments are good practice for all projects involving the processing of personal data. The GDPR states however that they must be carried out in certain circumstances;

- High risk processing of personal data, particularly involving new technologies
- Profiling with significant effects on individuals
- large scale special category/criminal data processing
- public surveillance on a large scale (for example CCTV of a publically accessible area)

The council has extensive Guidance and Procedures including Screening questions and DPIA templates for carrying out these assessments which are available on City People here.

8. International transfers

The GDPR requires that where personal data is transferred to a third country (non EU and EEA countries) those countries need to have been judged by the ICO as Adequate Countries or there needs to be necessary safeguards in place with the organisation. Safeguards such as a legally binding agreement between public bodies or contract clauses approved by the ICO. There is list of Adequate Countries on the ICO's website. There are exemptions to these

requirements although many are not available to public bodies such as the council when we are exercising their powers.

9. Further information, enquiries and complaints

Further information and guidance on data protection is available on the Information Commissioner's website at www.ico.org.uk

Advice on GDPR and the DPA can be sought and obtained from the Data Protection Officer or the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services team. They will be responsible for dealing with all internal and external enquires and are also the first point of contact on any of the issues mentioned in this Policy document.

An individual has the right to complain about the response they have received regarding their information right's request as well as to complain about other breaches of the GDPR and the DPA. All complaints should be written, dated and should include details of the complainant, as well as a detailed account of the nature of the problem.

Individuals under the right to be informed need to be provided (in the Privacy Notice) with the Data Protection Officer's contact details being dpo@lincoln.gov.uk and their right to complain to the Information Commissioner's Office and their contact details being: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 01625 545 700 www.ico.org.uk

10. Breach of the Policy

Any breach of this Policy must be investigated in line with the Data Protection Breach Management Policy and associated procedures. The council will always treat any data breach as a serious issue that could result in a disciplinary investigation.

The council encourages the notification of breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. Notification will also be taken into account in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach. Each incident will be investigated and judged on its individual circumstances in line with the Staff Code of Conduct or, in the case of elected members, the Members' Code of Conduct.

11. Data breach notification

The GDPR makes it mandatory for the council to report data breaches. A data breach is defined as;

'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, transmitted, stored or otherwise processed'.

Where the breach affects individuals' rights and freedoms. The council must report this to the Information Commissioner without delay and no later than within 72 hours.

If the risk to individual's rights and freedoms is high, the council, will also need to report the breach, without delay, to the individuals affected, for example the customers, partners or staff members to which the personal data relates.

The council has its own Data Breach Management Policy here and internal data breach reporting e-form system here.

Whether the breach is to be reported to the Information Commissioner or data subjects is a decision for the SIRO, Freedom of Information Officer/Legal and Democratic Services Manager and Data Protection Officer.

12. Policy Compliance

12.1. Compliance Measurement

The Council will ensure compliance with this Policy by regularly reviewing organisational and technological processes to ensure compliance with the GDPR and the DPA and in the provision of training for all staff and elected members processing personal data, which will be monitored and reported by the Information Governance Board and Audit Committee.

All policies and procedures relating to the GDPR and the DPA will be subject to scrutiny by the Policy Scrutiny Committee and the Audit Committee.

The Data Protection Officer will keep a record of all incidents and breaches relating to the GDPR and the DPA and will deal with all correspondence with the ICO relating to data protection matters.

IAO's will be asked to declare that they are compliant in their business areas with the GDPR and the DPA on an annual basis by submitting their IAO Checklist as required.

12.2. Non-Compliance

A deliberate or reckless breach of the GDPR or the DPA could result in a member of staff facing disciplinary action. Managers must ensure that all staff familiarise themselves with the content of this Policy.

All personal data recorded in any format must be handled securely and appropriately, and staff must not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff will be considered a disciplinary issue.

Employees should be aware that it is a criminal offence deliberately or recklessly to disclose personal data without the authority of council. It is also a criminal offence under DPA to re-identify personal data and processing this without the authority of the council and to alter personal data to prevent disclosure. In addition civil actions may be brought against individuals and the council for compensation.

Non-compliance of this Policy may also result in a report being made to the ICO which could result in council facing enforcement action, including substantial fines, in addition to substantial reputational damage.

12.3 Policy Review

This Policy will be reviewed every two years by Policy Scrutiny Committee and updated in the interim as required.

13. Related Policies, and Guidance

This Policy relates to other council policies, in particular:

Information Governance Strategy

Information Governance Policy

Legal Responsibilities Policy

Information Sharing Policy

Data Quality Policy

Data Protection Breach Management Policy

Freedom of Information Policy & Environmental Information Regulations Policy

Records Management Policy

Information Security Policy

Staff Code of Conduct

Member's Code of Conduct

Retention and Disposal Policy

14. Definitions

14.1. Abbreviations

Abbreviation	**Description**
DPA	Data Protection Act 2018
GDPR	General Data Protection Regulation
ICO	The Information Commissioner's Office
SIRO	Senior Information Risk Officer
IAO	Information Asset Owner

14.2. Definitions

Controller	A person who determines the purpose for which and the manner in which, Personal Data is to be processed. This may be an individual or an organisation and the processing may be carried out jointly with other persons
Data Subject	This is the living individual who is the subject of the Personal Data
Processor	A person who processes personal data on a Controller's behalf. Anyone responsible for the disposal of confidential waste is also included in this definition
Privacy Notice	A notice the council are required to give before collecting personal data from data subjects. The Privacy Notice must contain certain information. See Appendix 1
Profiling	Processing of personal data to evaluate certain aspects relating to data subjects in particular to analyse or predict behaviour, economic situation and personal preferences.
Information Commissioner's Office (ICO)	The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. www.ico.org.uk
Processing	Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data
Information Asset Owner (IAO)	Information Asset Owners within the Council are all Service Managers and where appropriate Team Leaders. IAO's are responsible for the data held in their areas. If you are unsure of your IAO contact the Data Protection Officer.
Information Asset Register	Part of the council's records of processing. This spreadsheet details the data we hold, where it is held, who can access it, the risks to the data, security measures, who the data is shared with. Each IAO is responsible for the section of Register relevant to their business

	area.
Pseudonymisation	Personal data which can no longer be attributed to a specific data subject without the use of additional information (kept separately and subject to security measures to ensure not attributed to data subject)
Legal Basis for processing personal data	- necessary for a contract - necessary for a legal obligation - vital interests (emergency to life) - **necessary for official authority/task carried out in the public interest (council's powers)** - necessary for legitimate interest (not available for council's powers) - OR the data subject has given consent
Additional Condition for processing special category data	Processing is necessary for:- - legal obligations in employment law, social security and social protection law - to protect vital interests (emergency to life) - carried out by a not-for-profit body with a political, philosophical, religious or trade union aim - relates to personal data made manifestly public by the data subject - for the establishment, exercise or defence of legal claims - public interest as permitted by law - preventative or occupational medicine - for reasons of public interest in the area of public health - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes - OR the data subject has given their explicit consent (written consent)
Examples of exemptions to the non-disclosure of third party personal data	- Crime and Taxation - National security - Defence - Prevention, detection and prosecution of criminal offences - Enforcement of civil matters - Disclosures required by law - Statement made by health, education and social care professionals
Examples of exemptions to the right of access.	- Legal professional privilege (legal advice)

	- Corporate finance- effecting markets and prices - Management forecasts - Negotiations - Confidential references in education training and employment - exemption is available to the organisation giving the reference not the organisation receiving the reference

What information must be supplied in a Privacy Notice?	Data obtained directly from data subject	Data not obtained directly from data subject (for example via a third party organisation)
Identity and contact details of the controller (the council) or the joint controllers (the council and others) and the data protection officer's contact details dpo@lincoln.gov.uk	✓	✓
Purpose of the processing and the lawful basis for the processing (see Definitions section)	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards, if applicable.	✓	✓
Retention period or criteria used to determine the retention period (see retention schedules)	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant (only where legal basis is Consent)	✓	✓
The right to lodge a complaint with the ICO	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of any automated decision making, including profiling and information about how decisions are made, the significance and the Consequences	✓	✓
When should information be provided?	At the time the data are obtained	Within a reasonable period of having obtained the data (within 1 month). If the data are used to communicate with the individual, at the latest, when the first communication takes place; or

		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Subject: The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

1. Introduction

- The General Data Protection Regulation (GDPR) will come into force on the 25th May 2018. The GDPR clarifies and strengths the rules on processing personal information (known as personal data) as first set out in the Data Protection Act 1998.
- The GDPR is expanded upon in the Data Protection Act 2018 (DPA) which also came into force in May 2018 and replaces the Data Protection Act 1998. Both the GDPR and DPA need to be read side by side.
- The idea behind GDPR is to allow individuals to take back control of their personal data and to update the data protection laws due to global technological developments.
- The Information Commissioner's Office (ICO) will be able to fine organisations up to 20 million Euros for non-compliance or 4% of global turnover whichever the greater, for non-compliance.
- This is a significant increase on previous fine levels.
- There have been recent high-profile cases reported in the media, regarding the loss or mishandling of personal data. This has focused attention on ensuring that personal data is appropriately handled within public bodies, and that the requirements of the data protection laws are being met.
- The council, handles a considerable amount of data, and therefore most council staff have some degree of exposure to personal data about customers and others.
- The council and all its staff have responsibilities to comply with the requirements of the GDPR and DPA. Failure to do so, could result in the council and/or its staff being criminally prosecuted and/or fined, as well as legal claims for compensation. This could also result in substantial reputational damage for the council.
- It is therefore important that all staff are familiar with the requirements of the new laws and clearly understand what they need to do on a day-to-day basis in order to comply.
- Council staff are granted access to systems, records, data and information on a "need to know" basis. Your access rights are tailored to your operational needs. Systems will trail and log system activity to the User ID and this ensures that only authorised staff can create, amend or delete data. In order to protect the accuracy and integrity of personal and other data you should only use your designated ID and **not** share it with other colleagues.
- The council has a **General Data Protection Regulation and Data Protection Policy** which is available via the council's Intranet site, on the dedicated Data Protection Page.
- This sheet is not a comprehensive guide and only covers the basics – see Section 4 below for details of additional sources of guidance and advice. **If you are in doubt, seek advice.**

2. What does the Act cover?

- In summary, the GDPR and DPA relates to:

    - Paper and manual records, as well as computer-based and electronic records;
    - Personal data of living individuals (who are known as **Data Subjects**);
    - Any person or organisation (known as **Controllers**) that holds data, about living individuals and determines how the personal data is used.
    - 6 principles relating to the collection, use, processing and disclosure of data that must be complied with by the **Controllers and Processors** acting on behalf of the council, who must be instructed under a contract which is complaint with the new laws;
    - In order to protect the **Data Subjects** there are defined rules about what types of disclosure of their information are permitted and those that are prohibited and the council and its staff must rigidly comply in respect of disclosure;
    - The rights of **Data Subjects have been extended** in relation to access to their personal data (referred to as a **Subject Access Request**). The council can no longer charge a fee for this and can no longer insist on a written request, but can encourage requesters

to use the council's online form. The time limit to respond to these requests has reduced to one calendar month to in some case 28 days. The council can still insist on proof of the requester's identity.

- This information must be provided in a legible form, with interpretations provided for any codes used and if the request is made electronically the response should be given in a commonly used electronic format and if available through self-service by the **Data Subject** to a secure online system.
- If, upon receiving the requested information held by the **Controller**, the **Data Subject** feels that it contains errors, he/she has the right to apply to rectification, restriction of its processing and erasure (deletion) of the affected personal data. **The GDPR has extended these rights** to include a right to data portability (to move data between organisations freely), a right to be informed of how their data is being used (privacy notices), a right to object to its use and rights related to automated decision making (decisions made solely by computers).
- If the **Data Subject** suffers damage by reason of any contravention by the **Data Controller** of any requirement of the GDPR or DPA, then he/she has the right to receive compensation. DPA has expanded this to include compensation for any adverse effect which is likely increase the number of compensation claims.

3. What do I need to do?

- Firstly, you must read this **Summary** and the GDPR and Data Protection Policy available on the council's intranet. If you don't have access to the intranet it is the responsibility of your line manager to ensure you receive a copy of this.
- Become familiar with the 6 DPA principles of processing personal data. In summary these are;
  1) process the data lawfully, fairly and transparently
  2) use the data only for the purpose it was provided for
  3) limit the amount of data to only what is needed
  4) ensure the data is accurate and up to date.
  5) only keep the data for as long as necessary
  6) keep the data secure and only disclose it to those who need to know.
- Consider how, in the course of your duties, you either collect, process, analyse, disclose or otherwise deal with personal data;
- You should advise anyone enquiring about accessing their personal data that the council holds, to complete the **Subject Access Request Form** and to forward it and an approved form of identity, to the council's Legal Officer, Karan Shearwood, who logs all requests. The **Subject Access Request Form** is available from the council's website. GDPR also allows requests to be made orally and therefore requests can also be made by contacting the council's Legal Officer at legal@lincoln.go.uk or telephone 01522 881188.
- You should advise anyone with a query regarding data protection to contact our Data Protection Officer at dpo@lincoln.gov.uk or telephone 881188.
- Think carefully about disclosing information to others, irrespective of whether the request is in person, in writing (including emails and faxes) or via the telephone. Remember that the DPA applies to manual records and paper files as well as electronic records and systems;
- Protect your system user identity and related passwords so that no one can access systems in your name:
  - Do not share your ID and password
  - Do not use another colleague's ID to access systems
  - Do not write down your passwords
  - **Any breach of Information Security Policies is a disciplinary offence.**
  - Choose combinations of letters, numbers and characters to provide more secure password combinations, and do not use more obvious passwords such as your birthday, car registration number or a pet's name;
- Only collect the personal data required for a particular operational purpose;
- When asked to disclose information ensure that the enquirer is entitled to access the data:
  - Is the person making the request proven to be the data subject?

  - Be certain that other colleagues working in your department and elsewhere in the council have the right to receive or view personal data **before** releasing any requested information. They may not share your level of access rights and may not "need to know". **If in any doubt consult with your line manager or team leader**;
  - Be aware that there are people who will try and trick you in to giving out personal data so always ensure that the individual making the request is entitled to view such data, **before** such data is revealed. Be aware that unauthorised disclosure of personal data is an offence and you could be held liable;
  - If in doubt about the identity and validity of the person making the request ask for the request to be made in writing and check that the request is not potentially bogus.
- Do not leave documents containing personal data exposed on your workspace where customers or other employees could read or remove them. Adopt a **'clear desk'** approach by securing and not displaying, hard copy personal data when it is not being used;
- Only dispose of confidential documents or information through the council's confidential waste paper service or by cross-cut shredding with the department;
- Lock your computer whenever you are leaving your desk ;
- Position your computer screen away from windows and corridors to prevent accidental disclosures of personal data;
- Use encryption on storage devices containing personal data that may be taken out of the office; and
- For computer systems not on the council network ensure that data is backed up and the copies are kept in a secure place.

4. Sources of Further Information

- **Information Commissioner's Website:** www.ico.gov.uk
- **The Data Protection Policies are available on City People**
- **Data Protection Officer:** Sally Brooks-ext. 3765
- **Freedom of Information Officer** and **Legal & Democratic Services Manager:** Becky Scott-ext 3441
- **Business Development & IT Manager:** Matt Smith-ext 3308

This page is intentionally blank.

Information Governance Policy

Document Control

Organisation	City of Lincoln Council
Title	Information Governance Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018 Executive
Filename	Information Governance Policy
Version	V.1.1
Protective Marking	Official
Next Review Date	July 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V 1.1	Becky Scott LDSM	June 2018	Updating policy in view of General Data Protection Registration ("GDPR") and new Data Protection Act 2018 ("the Act"), and amendments to roles

Table of Contents

1 Overview

This organisation collects and uses a wide range of information for many different purposes. As such, information is a vital asset that the organisation is reliant on, both for the provision and for the efficient management of services and resources. It is essential that there is a robust information governance management framework and policies to ensure that information is effectively managed and that the risks of loss of information confidentiality, integrity and availability are reduced.

The objectives of Information Governance are specifically:

Legal Compliance. To achieve the necessary balance between openness and security by complying with the relevant legislative requirements.

Information Security. To apply security measures that are appropriate to the contents of the information.

Information and Records Management. To ensure that the creation, storage, movement, archiving and disposal of information and records is properly managed.

Information/Data Quality. To support the provision of quality service delivery by the availability of quality information.

Information Sharing. To ensure that information can be effectively shared internally and between partner organisations while complying with the law and best practice standards.

Awareness and Guidance. To develop support arrangements which provide employees with awareness training and access to information governance policies and guidance.

2 Purpose

The purpose of this document is to set out the Information Governance Policy, including the Information Governance Management Framework, for City of Lincoln Council ("the Council"). It demonstrates management commitment to having in place sound information governance arrangements, gives clear direction to managers and staff, and will ensure that legal requirements and best practice standards are met.

3 Scope

This policy, framework and supporting policies apply to:

All data, information and records owned by the Council, but also including those held by contractors or partner organisations.

It applies to any information that is owned by other organisations, but may be accessed and used by Council employees, where there is no specific Information Sharing Agreement in place.

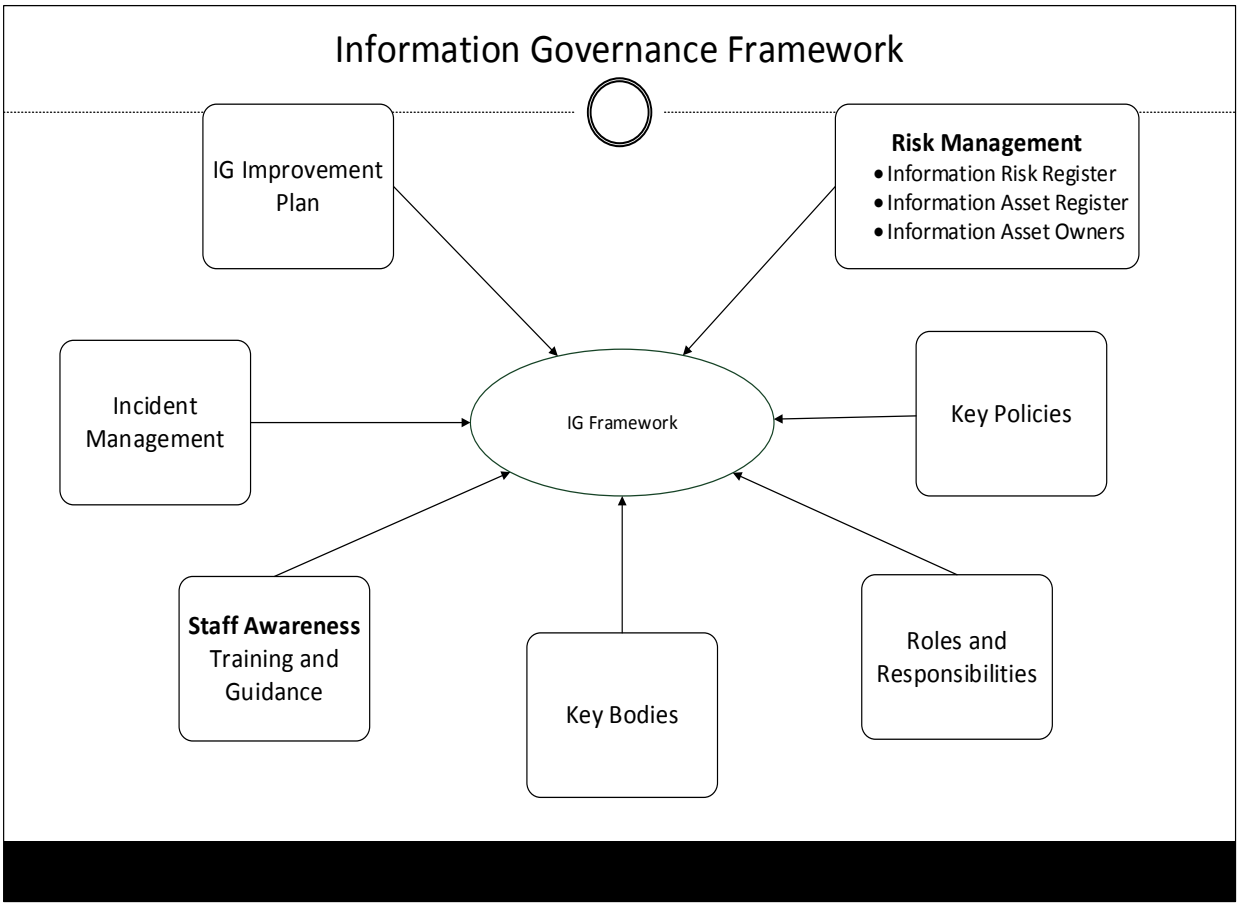
It applies to information in any storage format and however transmitted (including paper, voice, photo, video, audio or any digital format).

All employees of the council, and also council members, temporary workers, volunteers, student placements etc.

The employees of any other organisations having access to Council information; for example, auditors, contractors, and other partner agencies where there is no specific Information Sharing Agreement in place.

4 Policy

4.1 The Information Governance Management Framework



Note IG Improvement is the IG Action Plan

4.1.1 Risk Management

It is important that information risks are acknowledged, documented, assessed and managed through the Council risk management arrangements. This puts

information governance on the same footing as other corporate governance areas, and is reflected in its importance in the Senior Information Risk Owner's (SIRO) role.

4.1.2 Key Policies

An effective information governance structure is dependent on having key policies in place that cover three areas:

Information Compliance

Information Compliance is primarily concerned with the governance around, and the laws relating to, an organisation's information. It is also concerned with making sure information is of good quality and is properly and legally shared both internally and externally. The Council will make sure that there is:

a. An Information Governance Policy (this document) to set out a framework to manage its information governance responsibilities.

b. A Legal Responsibilities Policy to set out the main information-related legislation and the individual and collective responsibilities arising from it.

c. An Information Sharing Policy to cover any sharing of personal or confidential information with partner agencies or involving individual large transfers of such information. This Policy will make sure that an information sharing agreement based on a Council information sharing standard is in place and will set out the expected process and the standards of security and information handling.

d. A Data Quality Policy to set out the Council's standards to make sure that information is timely, comprehensive, accurate, complete, up-to date, accessible, and relates to the correct person. Key to this is that there will be validation of data at the point of collection wherever possible, and that there are procedures for the assessment of data quality that are independent of the source of data collection.

Information Rights

The main legislation applying to information rights is the Data Protection Act 2018 the Freedom of Information Act 2000, and the Environmental Information Regulations 2004. In addition, Common Law has established a "duty of confidence" requiring us to keep other categories of information such as intellectual property confidential. In order to make sure that the requirements of information law are covered there will be:

a. A Data Protection Policy setting out the seven principles that all users of Council information must be aware of and adhere to. The principles specify how personal information and sensitive personal information must be collected and managed to ensure the fair treatment of individuals and their personal information within the rights that are given under the Act.

The Act gives individuals the right to access their personal information. There are potentially severe penalties for any breach of the data protection principles. There is a Data Protection Breach Management Policy to provide assistance in the event of an incident.

b. A Freedom of Information Policy the sets out the Council's policy with respect to The Freedom of Information Act (FOI) which gives any individual the right of access to information held by the organisation. This is subject to some exemptions, most notably for personal information, as defined by the DPA. To comply with the law the Council must respond to any such request within 20 working days.

c. A Records Management Policy to make sure that information and records are effectively managed, and that the Council can meet its information governance objectives and which sets out the Council's standards for handling information during each phase of the information lifecycle; creation, use, semi-active use, and final outcome.

Information Security

Information security is concerned with the confidentiality, integrity and availability of information in any format. This is an important and challenging area since new technologies are changing both the way we work and how we expect to access and use information. The Council's reliance on information is so great that difficulties in this area could severely impact on our ability to deliver services. Consequently, there will be an Information Security Policy with supporting policies and guidance that will comply with the law, best practice and any current certification standards.

Other relevant policies and guidance are listed at Paragraph 6.

4.1.3 Information Governance Roles

These are the Senior Information Risk Owner, the Data Protection Officer, the Freedom of Information Officer and the Information Asset Owners.

The Senior Information Risk Owner (SIRO)

The SIRO will be a senior member of the management team, with an understanding how the strategic business goals of the organisation may be impacted by information risks.

Key tasks are to:

- Make sure that information risks are fully recognised in directorate and corporate risk registers.
- Take overall ownership of the risk assessment process for information risk, including review of an annual information risk assessment.
- Review and agree action in respect of identified information risks;

- Make sure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;

- Provide a focal point for the resolution and/or discussion of information risk issues; and

- Make sure the corporate management team is adequately briefed on information risk issues.

The Data Protection Officer - The Data Protection Officer is the representative from the senior level of management who acts as the overall Information Governance Lead and co-ordinate the information governance work programme. The post is required under the new GDPR and is therefore a statutory requirement.. They will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of information governance. They will provide a focal point for the resolution and/or discussion of information governance issues.

Key tasks are to:

- To inform and advise the Council and its staff/members who carry out processing of their obligations pursuant to data protection laws;

- To monitor compliance with data protection laws of the Council's data protection provisions and policies, in relation to the protection of personal data, including the assignment of responsibilities, awareness training and training staff/members involved in processing operations and the related audits;

- To provide advice where requested as regards the data protection impact assessment and monitor its performance.

- To co-operate with the Information Commissioner's Office (ICO)

- To act as a contact point for the ICO on issues relating to processing, including prior consultation where required and where appropriate with regard to any other matter.

Information Asset Owners

The Information Asset Owners (IAO) will be senior members of staff who are the nominated owners for one or more identified information assets of the Council. It is a core information governance objective that all information assets of the Council are identified and that their business importance is established.

The role of Information Asset Owners is to:

- Complete a six monthly asset owner checklist which outlines their responsibilities, and include; identifying and documenting the scope, importance and process map of all Information Assets they own. The Information Asset Owner checklist is attached at Appendix A.

- Take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks.

- Provide support to the SIRO and the IT and Information Governance Board (AD Group) to maintain their awareness of the risks to all information assets that are owned by the organisation and for the organisation's overall risk reporting requirements and procedures.

- Make sure that staff in their teams and relevant others are aware of and comply with expected information governance working practices for the effective use of owned Information Assets. This includes records of the information disclosed from an asset where this is permitted.

- Provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets.

- Make sure that the Council's information security incident policy requirements are applied to their information assets.

- Foster an effective information governance and security culture for staff and others who access or use the information assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with Council Policy.

- Set out local procedures that are consistent with corporate information security policies and guidelines.

Specialist Supporting Roles and Knowledge

There will be trained staff with specialist knowledge both to support the senior information roles, and to provide staff and managers with specific advice about the policies and guidance. The specialist knowledge covers information law (Data Protection and Freedom of Information Acts), information security, data quality, information and records management.

Service Managers

All managers will make sure that:

- The requirements of the information governance policy framework, its supporting policies and guidance are built into local procedures.

- That there is compliance with all relevant information governance policies within their area of responsibility.
- Information governance issues are identified and resolved whenever there are changes to services or procedures.
- Their staff are properly supported to meet the requirements of information governance and security policies and guidance, by ensuring that they are aware of:
    - The policies and guidance that apply to their work area.
    - Their responsibility for the information that they use.
    - Where to get advice on security issues and how to report suspected security incidents.

All Staff

All staff are responsible for:

- Making sure that they comply with all information governance policies and information security policies and procedures that are relevant to their service and consulting their manager if in doubt.
- Seeking further advice if they are uncertain how to proceed.
- Reporting suspected data protection breaches/information security incidents.

4.1.4 Key Bodies

The Information Governance Strategy has been approved by the Assistant Directors Group who also sit as the Information Governance Board. They will receive updates at least every 3 months.

Audit Committee have changed their Terms of Reference to include a role of overseeing Information Governance and progress against the action plan. The Chair has taken on the role as lead Information Governance member and the committee will receive reports on a bi-annual basis.

4.1.5 Staff Awareness

- Staff awareness is a key issue in achieving both compliance with information governance policies and the improvements required by the improvement plan. Accordingly there will be.
- Mandatory base line training in key information governance competencies for all staff will take place every two years.

- Additional training for all employees routinely handling 'sensitive personal information', as defined by the DPA 2018.

- All information governance policies and guidance to be available on the Intranet/City People.

- Staff with specialist knowledge available to provide advice across the full range of information governance areas.

4.1.6 Data Protection Breach Management Policy

There will be a Data Protection Breach Management Policy and procedures that set out how incidents will be reported and managed. The results of incident investigations will be reported to the information governance working group and to the Information Governance Board (AD Group)

4.1.7 Information Governance Action Plan

There will be an information governance action plan that identifies the detailed requirements necessary to achieve compliance with the main policy objectives. This plan will be monitored and progressed by the information governance working group to ensure that there continuing development. Progress against the plan will be reported quarterly to the Information Governance Board (AD Group), and bi-annually to Audit Committee.

5 Policy Compliance

5.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements, such as those required by the Data Protection Act 2018 and the Freedom of Information Act 2000 and Environmental Information Regulations 2004, these are detailed in the Council's relevant Policies.

All Policies relating to information management will be subject to scrutiny by the Policy Scrutiny Committee and/or the Audit Committee.

5.2 Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

5.3 Policy Review

This Policy will be reviewed every two years and updated in the interim as required.

6 Relevant Legislation, Standards, Policies, and Guidance

The primary legislation governing the Council's information management activities is described in the Legal Responsibilities Policy.

Legal Responsibilities Policy

Document Control

Organisation	City of Lincoln Council
Title	Legal Responsibilities Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018 - Executive
Filename	Legal Responsibilities Policy
Version	V.1.1
Protective Marking	Not Protectively Marked
Next Review Date	July 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V 1.1	Becky Scott LDSM	June 2018	Updating policy in view of General Data Protection Registration ("GDPR") and new Data Protection Act 2018 ("the Act"), and amendments to roles

Table of Contents

1 Overview

This Policy lists and describes the legislation and regulations that govern information management and highlights the risks both to the organisation and to individuals for failing to comply.

2 Purpose

At City of Lincoln Council ("the Council") we create, collect, hold, and use vast amounts and types of information to carry out our functions, much of which is governed by legislation. For instance, we process personal data about people and organisations with whom we deal with, information protected by copyright, and intellectual property which we must keep confidential.

In addition, we are occasionally required by law to collect and use certain types of personal information to comply with the requirements of Government departments.

However, we also make much of our information publically available to demonstrate open and transparent government and Information Rights legislation such as the Freedom of Information Act 2000 sets out how we must publish or respond to legitimate requests for our information.

This Policy details our responsibilities under the wide and varied legislation that governs our information and information systems.

3 Scope

Any information must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer, or recorded on other media. For instance, there are safeguards set out in the Data Protection Act 2018 to make sure that personal information is collected and processed correctly.

This Policy relates to all information held or processed by the Council. It applies to all full time and part time employees of the Council, elected members, partner agencies, contracted employees, third party contractors (including agency employees), volunteers and students or trainees on placement with the Council, who have access to information held or processed by the Council.

4 Roles and Responsibilities

For most information-related legislation the following Council officers are accountable and responsible for compliance. Where specific responsibilities exist for legislation, these are included within the description of the particular legislation below.

- **Chief Executive**. The Chief Executive has overall responsibility for strategic and operational management, including making sure that Council policies comply with all legal, statutory and good practice guidance requirements.

- The Data Protection Officer's role is defined by the GDPR and includes;
- To inform and advise the Council and its staff/members who carry out processing of their obligations pursuant to data protection laws;
- To monitor compliance with data protection laws of the Council's data protection provisions and policies, in relation to the protection of personal data, including the assignment of responsibilities, awareness training and training staff/members involved in processing operations and the related audits;
- To provide advice where requested as regards the data protection impact assessment and monitor its performance.
- To co-operate with the Information Commissioner's Office (ICO)
- To act as a contact point for the ICO on issues relating to processing, including prior consultation where required and where appropriate with regard to any other matter.

- Directors and Assistant Directors are responsible for ensuring compliance with this Policy and all relating Council polices and aiding the process of making all staff aware of the Council's legal responsibilities within their directorates.
- Information Asset Owners are responsible for ensuring that all staff in the business areas they have responsibility for have processes and procedures in place to comply with this and relating polices and that all new staff receive an induction briefing on particular legislation where required.
- All staff full time and part time, elected members, partner agencies, contracted employees and third party contractors (including agency employees) volunteers and students or trainees on placement with the Council must comply with this Policy and all Council polices relating to the Council's legal responsibilities.
- The responsibility for providing day-to-day advice and guidance to support the Council in complying with this policy and its legal responsibilities rests with the City Solicitor and the Legal & Democratic Services Manager and the Legal Services team.

5 Policy

This section lists the legislation applicable to information and information systems and details specific responsibilities for complying with it.

5.1 Civil Contingencies Act 2004

Category 1 organisations (the emergency services, local authorities, NHS bodies) are at the core of the response to most emergencies and are subject to the full set of civil protection duties.

The Act requires that, as Category 1 Responders, Local Authorities put in place Business Continuity Management arrangements.

5.1.1 What will the Council do?

In order to meet its obligations under the Act, the Council will:

- Assess the risk of emergencies occurring and use this to inform contingency planning.
- Put in place emergency plans.
- Put in place business continuity management arrangements.
- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency.
- Share information with other local responders to enhance co-ordination.
- Co-operate with other local responders to enhance co-ordination and efficiency.

5.1.2 What will the Council's employees do?

Council employees and other parties listed at paragraph three will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.2 Companies Act 2006

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

5.2.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies and procedures and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.2.2 What will the Council's employees do?

Council employees and other parties listed at paragraph three will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.3 Common Law of Confidentiality

Common Law of Confidentiality is not in any written Act of Parliament. It is "common" law which means that it has been established over a period of time through the courts.

The law recognises that some information has a quality of confidence, which means that the individual or organisation that provided the information has an expectation that it will not be shared with or disclosed to others.

For information to have a quality of confidence it is generally accepted that:

- it is not "trivial" in its nature;
- it is not in the public domain or easily available from another source;
- it has a degree of sensitivity; and
- it has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence. For example information shared between a solicitor/client, health practitioner/patient, etc.

However, as with the Human Rights Act 1998, confidentiality is a qualified right. Qualified Rights are rights which can be restricted not only in times of war or emergency but also in order to protect the rights of another or the wider public interest. In general, qualified rights are structured so that the first part of the Article sets out the right, while the second part establishes the grounds on which a public authority can legitimately interfere with that right in order to protect the wider public interest

The Council is able to override a duty of confidence when it is required by law, or if it is in the public interest to do so.

5.3.1 What will the Council do?

In order to meet its obligations under the Common Law of Confidentiality, the Council will make sure that:

- Confidentiality is included as an essential element of employee terms and conditions.
- The need to keep information confidential where appropriate is included in all security awareness training.

- Confidentiality clauses are included in all Council contracts where information may be accessed or shared.

5.3.2 What will the Council's employees do?

Council employees and other parties listed at paragraph three will recognise and understand the importance of not disclosing confidential information to anyone who does not have a "need to know" and will comply with Council's policies and procedures relating to this legislation.

5.3.3 Roles and Responsibilities

Everyone who comes into contact with information has a responsibility to keep it private where necessary and in some cases may be held personally accountable for any breach of confidentiality.

5.4 Computer Misuse Act 1990

The Computer Misuse Act makes it illegal to gain unauthorised access to a computer. The Act is made up of three separate offences:

- Unauthorised access to computer material; the act of accessing materials without authorisation is an offence even if no damage is done, files deleted or changed
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material; including the amendment, damage of data, including the introduction of computer viruses.

5.4.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies and procedures and that any policy or specific requirements and the penalties for offences under the Act are included in awareness training provided to staff, Members and partners.

5.4.2 What will the Council's employees do?

As well as not committing any of the three basic offences, Council employees and other parties listed at paragraph must not:

1. Display any information which enables others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate hacking)

2. Display any information that may lead to any unauthorised modification of computer materials (such modifications would include activities such as the circulation of "infected" software or the unauthorised addition of a password)

3. Display any material, which may incite or encourage others to carry out unauthorised access to or modification of computer materials.

5.4.3 What are the consequences of non-compliance?

The penalties for committing criminal offences in each of the three categories are as follows:

1. Unauthorised access to computer material (basic hacking) including the illicit copying of software held in any computer which carries a penalty of up to six months imprisonment or up to a £5,000 fine.

2. Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking which carries a penalty of up to five years of imprisonment and an unlimited fine.

3. Unauthorised modification of computer material, which includes:

   i) intentional and unauthorised destruction of software or data.

   ii) the circulation of "infected" materials online.

   iii) An unauthorised addition of a password to a data file.

This offence carries a penalty of up to five years of imprisonment and an unlimited fine.

5.5 Copyright, Designs and Patents Act 1988

The law gives the creators of literary, dramatic, musical, artistic works, sound recordings, broadcasts, films and typographical arrangement of published editions, rights to control the ways in which their material may be used.

The rights cover; broadcast and public performance, copying, adapting, issuing, renting and lending copies to the public.

In many cases, the creator will also have the right to be identified as the author and to object to distortions of his work. International conventions give protection in most countries, subject to national laws.

5.5.1 Types of work protected

1. **Literary**. Song lyrics, manuscripts, manuals, computer programs, commercial documents, leaflets, newsletters & articles etc.

2. **Dramatic**. Plays, dance, etc.

3. **Musical**. Recordings and score.

4. **Artistic**. Photography, painting, sculptures, architecture, technical drawings/diagrams, maps, logos.

5. **Typographical arrangement of published editions**. Magazines, periodicals etc.

6. **Sound recording**. May be recordings of other copyright works, e.g. musical and literary.

7. **Film**. Video footage, films, broadcasts and cable programmes.

The Copyright (Computer Programs) Regulations 1992 extended the rules covering literary works to include computer programs.

Only software that is developed by the Council, or either licensed or provided by a developer to the Council should be used.

The copyright of all software developed within the Council by staff or contractors should be held by the Council.

The right of the Council to make copies, for its own use, of any software provided must be retained by the Council.

Under no circumstances should software be copied from one machine to another without the appropriate licence agreement. Only staff authorised by IT Services may install, or move software.

5.5.2 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.5.3 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation. Specifically, employees and other authorised users of the Council's ICT equipment will not install or use software, or use images, media or other copyrighted material that has not been approved and/or licensed for Council use.

5.5.4 What are the consequences of non-compliance?

Copyright infringement that may be criminal offences under the Copyright, Designs and Patents Act 1988 are the:

- Making copies for the purpose of selling or hiring them to others;

- Importing infringing copies (except for personal use);

- Offering for sale or hire, publicly displaying or otherwise distributing infringing copies in the course of a business;
- Distributing a large enough number of copies to have a noticeable effect on the business of the copyright owner;
- Making or possessing equipment for the purposes of making infringing copies in the course of a business;
- Publicly performing a work in knowledge that the performance is unauthorised;
- Communicating copies or infringing the right to "make available" copies to the public (either in the course of a business, or to an extent prejudicial to the copyright owner); and
- Manufacturing commercially, importing for non-personal use, possessing in the course of a business, or distributing to an extent that has a noticeable effect on the business of the copyright holder, a device primarily designed for circumventing a technological copyright protection measure.

The penalties for these copyright infringement offences may include:

- Before a magistrates' Court, the penalties for distributing unauthorised files are a maximum fine of £5,000 and/or six months imprisonment;
- On indictment (in the Crown Court) some offences may attract an unlimited fine and up to 10 years imprisonment.

5.6 Data Protection Act 2018

The Act gives rights to individuals about whom personal data is recorded (Data Subjects). They may obtain personal data held about themselves, challenge it if appropriate and claim compensation in certain circumstances. The Act places obligations on those who record and use personal data (Data Users). They must be open about that use (through the data protection register) and follow sound and proper practices (the Data Protection principles). Any requests to view or receive personal data must be in line with the Data Protection Policy and guidance

The Act applies to personal data and is based upon a set of eight principles, which should form the basis of good organisational practice. The principles state that personal data:

1. Shall be processed lawfully fairly and in a transparent manner.
2. Shall be collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes.

3. Shall be adequate, relevant and limited to what is necessary.

4. Shall be accurate and where necessary, kept up to date.

5. Shall be kept in a form which permits identification of data subjects for no longer than necessary.

6. Processed in a manner that ensures appropriate security of the personal data.

7. The Council shall be responsible for and be able to demonstrate compliance with the principles.

5.6.1 What will the Council do?

In order to meet its obligations under the Data Protection Act, the Council will make sure that:

- There is an individual with specific responsibility for data protection in the organisation, namely the Chief Executive, with support from the Senior Information Risk Owner and the Data Protection Officer/City Solicitor.

- Everyone managing and handling personal information understands that they are legally responsible for following good data protection practice.

- Everyone managing and handling personal information is properly trained to do so and adequate advice and guidance is available.

- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.

- Methods of handling personal information are regularly assessed and evaluated.

- All actual or potential breaches of the Data Protection Act are investigated, mitigated, and reported as appropriate.

5.6.2 What will the Council's employees do?

Employees and agents of the Council are personally responsible for complying with the Data Protection Act. In particular they will make sure that:

- They attend or complete data protection training provided by or on behalf of the Council.

- When collecting or processing personal information in the course of their duties they follow any policies, guidance, and procedures provided by the Council for that purpose.

- They report any breaches of the Act using the Council's Data Protection Breach Management Policy.

- Queries about handling personal information are promptly and courteously dealt with.

5.6.3 What are the consequences of non-compliance?

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice of up to 20 million Euros or 4% of global turnover whichever the greater on a data controller.

5.6.4 Roles and Responsibilities

- The **Chief Executive** has overall responsibility for strategic and operational management, including ensuring that Council policies comply with all legal, statutory and good practice guidance requirements.

- The implementation of, and compliance with the Act is delegated to the **Council's Senior Information Risk Owner**.

- The **Council's Data Protection Officer** will provide guidance and advice to employees to facilitate the correct handling of personal information and to enable the Council to meet its legal obligations under the DPA.

- The **Council's Data Protection Officer** is responsible for notifying the Information Commissioner's Office of the Council's purposes for processing personal information.

- **Directors** and Assistant Directors are responsible for ensuring that the Council's Data Protection procedures are communicated and implemented within their directorates.

- **Information Asset Owners** are responsible for ensuring that all their staff are appropriately trained with regards to Data Protection and for ensuring that any Data Protection related issues in their own area are handled in compliance with this policy and relevant procedures.

- **Information Asset Owners** are responsible for ensuring that all personal data is disposed of securely and in line with the Retention and Disposal Policy.

- All **Council employees** must complete relevant Data Protection training.

- All **Council employees** are responsible for understanding, and adhering to this Policy and the Council's Policy and procedures relating to Data Protection.

- All **Council employees** should seek Data Protection advice from the Council's City Solicitor/Data Protection Officer, the Legal & Democratic Services Manager or the Legal Services team when necessary.

5.6.5 Sharing Personal Information with other Organisations

Personal information must not be disclosed to any other person or organisation via any insecure method.

Where such information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Agreement.

The Council's Data Protection Officer is responsible for the Information Sharing Agreements.

5.7 Environmental Information Regulations 2004

The Environmental Information Regulations provide members of the public with the right to access environmental information held by public authorities.

Environmental information covers:

- The state of the elements of the environment, such as air, water, soil, land, fauna (including human beings).
- Emissions and discharges, noise, energy, radiation, waste and other such substances.
- Measures and activities such as policies, plans and agreements affecting or likely to affect the state of the elements of the environment.
- Reports, cost-benefit and economic analyses.
- The state of human health and safety and contamination of the food chain.
- Cultural sites and built structures (to the extent they may be affected by the state of the elements of the environment).

The Council is required to respond to a request for environmental information within 20 working days although further reasonable details can be requested to identify and find the information in line with the legislation.

5.7.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.7.2 What will the Council's employees do?

Council employees and other parties listed at paragraph three of this policy will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.8 Freedom of Information Act 2000

Gives a general right of access to all types of recorded information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities.

Subject to the exemptions, any person who makes a request to a public authority for that information must be informed whether the public authority holds that information. If it does, that information must be supplied, subject to certain conditions.

Every public authority is required to adopt and maintain a publication scheme setting out how it intends to publish the different classes of information it holds, and whether there is a charge for the information.

Two Codes of Practice issued under the Act (under sections.45 and 46) provide guidance to public authorities about responding to requests for information, and records management which are available on the ICO website. The Act is enforced by the Information Commissioner.

5.8.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.8.2 What will the Council's employees do?

Council employees and other parties listed at paragraph three of this policy will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.8.3 What are the consequences of breaching the Act?

The Council may be breaching the Freedom of Information Act if it does any of the following:

- Fail to respond adequately to a request for information;
- Fail to adopt the model publication scheme, or do not publish the correct information.

- Deliberately destroy, hide or alter requested information to prevent it being released.

This last point is the only criminal offence in the Act that individuals and public authorities can be charged with.

Other breaches of the Act are unlawful but not criminal. The Information Commissioner's Office (ICO) cannot fine the Council if it fails to comply with the Act, nor can it require us to pay compensation to anyone for breaches of the Act. However, we should correct any mistakes as soon as we are aware of them.

5.9 Human Rights Act 1998

An individual's privacy and protection of property rights must be respected. This includes ensuring the security of personal data. Infringements could lead to breaches of these rights.

An employee's privacy is, however, subject to the provisions of the **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

5.9.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.9.2 What will the Council's employees do?

Council employees and other parties listed at paragraph three of this Policy will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.10 Privacy & Electronic Communications (EC Directive) Regulations

The Privacy and Electronic Communications Regulations (PECR) originally came into force in 2003 and were amended in 2004, 2011, and again in 2015. The regulations sit alongside the Data Protection Act and give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- Marketing calls, emails, texts and faxes.
- Cookies (and similar technologies).
- Keeping communications services secure.

- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

5.10.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.10.2 What will the Council's employees do?

Council employees and other parties listed at paragraph three will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.10.3 What are the consequences of not complying with the Regulations?

The regulations carry a number of sanctions for non-compliance. These are enforced by the ICO and include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice imposing a fine of up to 20 million Euros or 4 % of global turnover whichever the greater.

5.11 Re-use of Public Sector Information Regulations 2015

The Regulations are concerned with the re-use by businesses and citizens of information held by public sector bodies. "Re-use" essentially means the use of existing information in new products and services. Its aim is to support technology driven growth and civil society applications, for example, in the use of mapping information in satellite navigation products.

The Regulations affect how information can be re-used once it has been legitimately accessed, by placing obligations on the public sector to the benefit of re-users.

The Regulations do not create rights of access to information. They do not override or modify data protection rules. Re-use of public sector information in the UK must therefore comply with the Data Protection Act and any related regulations

5.11.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.11.2 What will the Council's employees do?

Council employees and other parties listed at paragraph 3 of this Policy will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.12 Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA is the law governing the use of covert techniques by public authorities. It requires that when public authorities, such as the police or government departments, need to use covert techniques to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights.

RIPA's guidelines and codes apply to actions such as:

- Intercepting communications, such as the content of telephone calls, emails or letters;
- Acquiring communications data: the 'who, when and where' of communications, such as a telephone billing or subscriber details;
- Conducting covert surveillance, either in private premises or vehicles (intrusive surveillance) or in public places (directed surveillance);
- The use of covert human intelligence sources, such as informants or undercover officers; and
- Access to electronic data protected by encryption or passwords.

RIPA applies to a wide-range of investigations in which private information might be obtained. Cases in which it applies include:

- Terrorism
- Crime
- Public safety
- Emergency services

5.12.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.12.2 What will the Council's employees do?

Council employees and other parties listed at paragraph 3 of this Policy will, where appropriate, comply with Council's policies and procedures relating to this legislation.

6 Policy Compliance

6.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements required by the Data Protection Act 1998 and the Freedom of Information Act 2000 and Environmental Information Regulations 2004 these are detailed in the Council's relevant Policies.

All Policies relating to information management will be subject to scrutiny by the Policy Scrutiny Committee and/or the Audit Committee.

6.2 Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

If any user is found to have breached this Policy, they will be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the Data Protection Officer being the City Solicitor, the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team.

6.3 Policy Review

This Policy will be reviewed every two years and updated in the interim as required.

7 Related Standards, Policies, and Processes

- Information Governance Policy
- Data Protection Policy
- Freedom of Information and Environmental Information Regulations Policy.
- Information Sharing Policy

- Data Quality Policy
- Data Protection Breach Management Policy
- Records Management Policy
- Information Security Policy
- Retention and Disposal Policy

8 Definitions

Information Asset Owner	The IAO was established by the Security Policy Framework. Their role is to protect and manage information held in the Council, and ensure that its value to the organisation is recognised. They are also responsible for promoting and fostering a culture of security of data within their teams and wider organisations. They also are required to complete an IAO checklist every six months. Information Asset Owners within the Council are all Service Managers and where appropriate Team Leaders.

This page is intentionally blank.

Information Sharing Policy

Document Control

Organisation	City of Lincoln Council
Title	Information Sharing Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018 - Executive
Filename	Information Sharing Policy
Version	V.2.1
Protective Marking	Not Protectively Marked
Next Review Date	July 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V.2.0	Sally Brooks	27/05/16	Change of flow chart and minor wording on factors to consider before sharing information.
V 2.1	Becky Scott LDSM	June 2018	Updating policy in view of General Data Protection Registration (“GDPR”) and new Data Protection Act 2018 (“the Act”), and amendments to roles

Table of Contents

Overview

Information sharing is key to City of Lincoln Council's ("the Council") goal of delivering better and more efficient services that are coordinated around the needs of the individual. Sharing information both internally and with our partners is essential to support early intervention and preventative work, for safeguarding and promoting welfare and for wider public protection. Information sharing is a vital element in improving outcomes for all.

The Council understands that it is most important that people remain confident that we keep their personal information safe and secure and that staff maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that all staff are aware of how they can share information appropriately as part of their day-to-day responsibilities and do so confidently.

1 Purpose

The purpose of this policy is to:

- Provide a framework for the Council and those working on its behalf to:
    - Provide information to deliver better services;
    - Consider the controls needed for information sharing; and
    - Make sure that partners sharing information are aware of the Council's Minimum Security Standards for securing information; the obligations

of consent; and how to take appropriate account of an individual's objection to the sharing.

- Establish a mechanism for the exchange of information between the Council and other **organisations**.

2 Scope

This Policy applies to all staff and members including those who are responsible for managing partnerships where information will be shared and those who are responsible for creating or providing the information that is to be shared.

Information sharing, in the context of this policy, means the disclosure of personal information from one or more organisations to a third party organisation or organisations. Information sharing can be:

- A reciprocal exchange of data;
- One or more organisations providing data to a third party or parties;
- Several organisations pooling information and making it available to each other;
- Several organisations pooling information and making it available to a third party or parties.
- Exceptional, one-off disclosures of data in unexpected or emergency situations.

Sharing non-personal information with other organisations. This is where the Council shares key information with other organisations to: improve customer experience; facilitate commissioning of services; manage and plan future services; assure and improve the quality of services; statutory returns and requests; to train staff; to audit performance.

Sharing personal information with other organisations. As long as it is necessary and proportionate, the Council can share personal information with other organisations: to prevent crime; to investigate complaints or potential legal claims; to protect children and adults at risk; to assess need and service delivery.

This policy covers two main types of information sharing. These are explained in more detail in Para 3:

- "Systematic", routine information sharing where the same data sets are shared between the same organisations for an established purpose; and
- Exceptional, one-off decisions to share information for any of a range of purposes.

3 Policy

3.1 Factors to consider before sharing information

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) staff and members must consider firstly whether there is a legal power (a legal gateway) either expressed or implied by legislation to share.

If staff are unsure about this they must seek advice from the Data Protection Officer or the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team.

If the answer is the above question is yes, staff must then consider what the sharing is meant to achieve and there should be a clear objective, or set of objectives. Being clear about this will identify the following:

- Could the objective be achieved without sharing the data or by anonymising it? It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

- What information needs to be shared? You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives.

- Who requires access to the shared personal data? You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- When should it be shared? It is good practice to document this, for example setting out whether the sharing should be an ongoing, routine process or whether it should only take place in response to particular events.

- How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- How can we check the sharing is achieving its objectives? You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- How do we make individuals aware of the information sharing? Consider what to tell the individuals concerned. Is their consent needed? Should the individuals be provided with a Privacy Notice, notifying them of who you are going to share their data with? Do they have an opportunity to object? How do you take account of their objections? How do you ensure the individual's rights are respected and can be exercised e.g. how can they access the

information held once shared? Is there any onward sharing necessary to a third party and if so, what are the restrictions needed on this, such as any further consent required?

- What risk to the individual and/or the organisation does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

In all circumstances of information sharing, staff will make sure that:

- When information needs to be shared, sharing complies with the law, guidance and best practice;
- The information must processed lawfully and fairly to comply with the DPA and the ICO's Code of Practice on Data Sharing published under section 52 of the DPA must be followed. This Policy has been written in accordance with the Code although further information on the Code can be found on the ICO's website www.ico.org.uk
- The sharing must not contravene other laws such as Article 8 of the Human Rights Act 1998 being The Right to Privacy.
- Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it.
- Individuals' rights will be respected, particularly regarding the confidentiality and security of their personal information and the sharing must not contravene laws such as the Common Law of Confidentiality.
- Confidentiality will be maintained unless there is a robust public interest or a legal justification in disclosure.
- They undertake reviews of information sharing to make sure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

3.2 Information Sharing Agreements

Information Sharing Agreements – sometimes known as 'Information or data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

An Information Sharing Agreement must at least document the following:

- The purpose, or purposes, of the sharing.

- The legal basis for sharing.
- The potential recipients or types of recipient and the circumstances in which they will have access;
- Who the data controller(s) is and any data processor(s).
- The data to be shared.
- Data quality – accuracy, relevance, usability.
- Data security.
- Retention of shared data.
- Individuals' rights – procedures for dealing with access requests, queries and complaints.
- Review of effectiveness/termination of the sharing agreement.
- Any particular obligations on all parties to the agreement, giving an assurance around the standards expected.
- Sanctions for failure to comply with the Agreement or breaches by individual staff.

3.3 Data Privacy Impact Assessments

Before entering into any information sharing arrangement, it is a legal requirement to carry out a Data Privacy Impact Assessment where the processing is likely to result in a high risk to the rights and freedoms of individuals and in particular in the following circumstances:-

- A systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual.
- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
- A systematic monitoring of a publically accessible area on a large scale.

In all other projects where there is potentially data sharing, the initial screening questions in the Data Privacy Impact Assessment should be carried out. This will help to assess the benefits that the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, or causing distress or embarrassment to individuals.

As well as harm to individuals, staff should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be. Further information on Data Privacy Impact Assessments can be found on the Council's Intranet

4 Policy Compliance

4.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements, such as those required by the DPA and the Freedom of Information Act 2000 and Environmental Information Regulations 2004, these are detailed in the Council's relevant Policies.

All Policies relating to information management will be subject to scrutiny by the Policy Scrutiny Committee and/or the Audit Committee.

4.2 Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

Where personal information is being shared a breach of this Policy could result in a breach of the DPA, for which the Council could face substantial fines, reputational damage and civil claims, and there could be possible criminal sanctions against individuals.

If any user is found to have breached this Policy, they will be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

The Council encourages the notification of Data Protection breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. Notification will also be taken into account in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach.

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the Data Protection Officer or the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team.

4.3 Policy Review

This Policy will be reviewed every two years and updated in the interim as required.

5 Related Standards, Policies, and Processes

-Information Governance Policy

-Legal Responsibilities Policy

-Data Protection Policy

-Data Quality Policy

-Data Protection Breach Management Policy

-Freedom of Information Policy & Environmental Information Regulations Policy

-Records Management Policy

-Information Security Policy

-Retention and Disposal Policy

6 Definitions

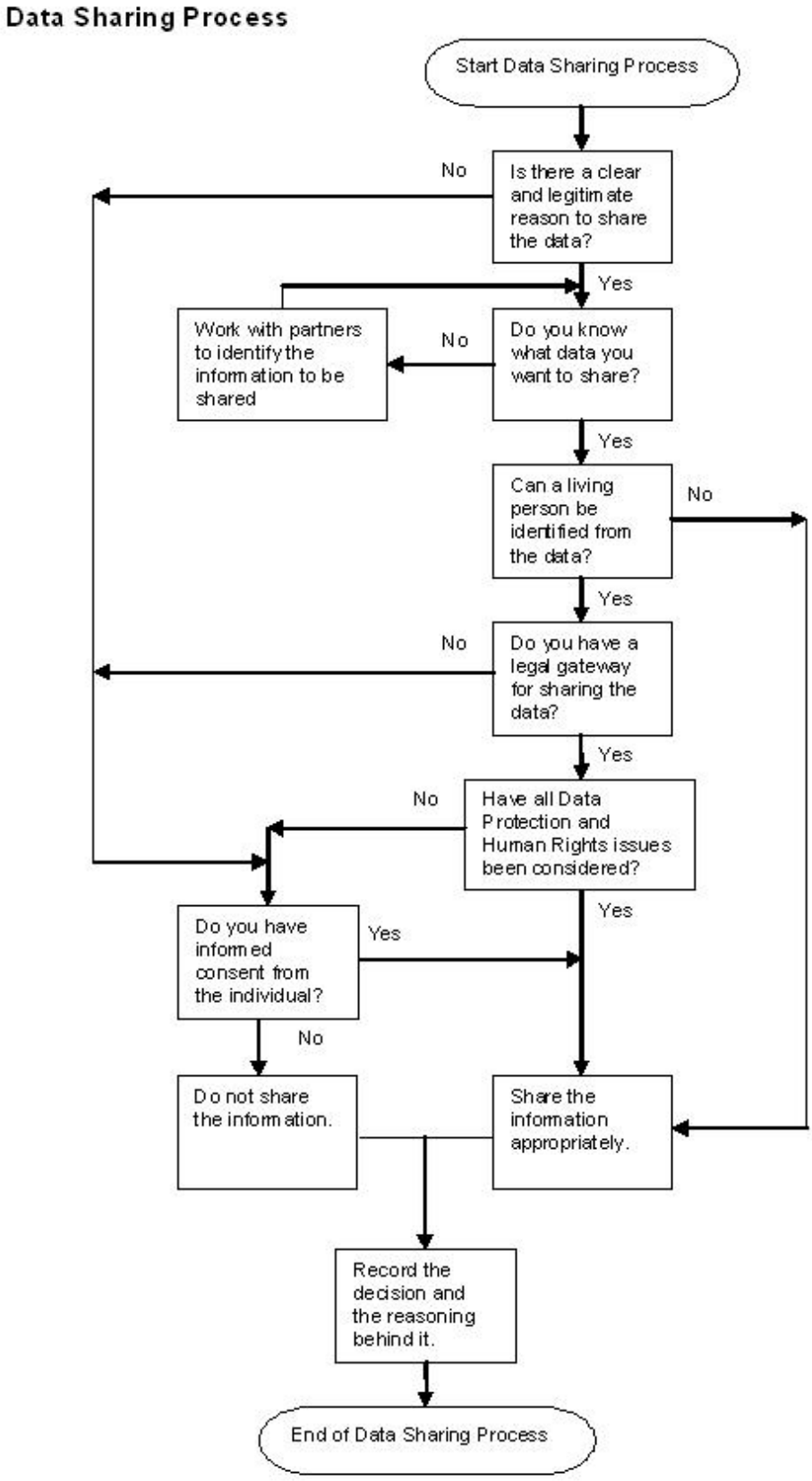
6.1 Definitions

Data Sharing	The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.
Data Controller	A data controller is the “person” recognised in law (i.e. an individual; organisation; or other corporate and unincorporated body of persons) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

Data Sharing Agreements	Set out a common set of rules to be adopted by various organisations involved in a data sharing operation.
Privacy Impact Assessments	A formalised document which shows the possible threats to privacy which could arise from a business activity.
Data Quality	Data quality relates to the accuracy, integrity, completeness and reliability of data and information.
Data Security	The policies, procedures and practices required to maintain and provide assurance of the confidentiality, integrity and availability of information.
Information	*"Information is data imbued with meaning and purpose". Anon* Information is something which tells us something and can also be communicated to someone else in a meaningful way. Information is data that is put into context, can be comprehended, understood and shared with other people and / or machines.
Retention	Means the length of time for which records are to be kept. Thus it normally represents and will be expressed as a disposal period.
ICO-Information Commissioner's Office	The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. www.ico.org.uk

Personal Data	Defined in s(1) of the DPA, as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' (the Council is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual. At least one of the conditions in Schedule 2 to the DPA must be met to process personal data.
Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing.
Processed fairly and lawfully	Data must be processed in accordance with the 3 provisions of the DPA. These are the data protection principles, the rights of the individual, and notification.
Privacy Notice	As a minimum, a Privacy Notice should tell people who you are, what you are going to do with their information and how it will be shared with. However it can also tell people more than this. It can for example provide information about people's rights of access to their data or your arrangements for keeping their data secure. Whatever you include in your Notice, its primary purpose is to make sure that information is collected and used fairly.

Appendix 1 – Flowchart of Key Questions for Information Sharing



Source: Centre of Excellence for Information Sharing http://informationsharing.org.uk/our-work/tools/scoping/how-do-we-decide-the-legal-basis-for-sharing/

This page is intentionally blank.

Data Quality Policy

Document Control

Organisation	City of Lincoln Council
Title	Data Quality Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018 - Executive
Filename	Data Quality Policy
Version	V.1.1
Protective Marking	Official
Next Review Date	May 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V1.1	Becky Scott LDSM	July 2018	Updated in view of the General Data Protection Regulation (“GDPR”) and the DPA 2018 (“the Act”) and amendments to role

Table of Contents

1 Overview

This policy sets out City of Lincoln Council's approach to data quality. It is a key element of the Council's Information Governance Framework. Data is one of our most important assets - it is extremely important as we want to be sure that information on which we base decisions and inform our planning is robust.

The data held by the Council is subject to all legislation affecting the creation and processing of data. This includes but is not limited to:

- The Data Protection Act 2018
- The General Data Protection Regulation EU (2016)
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- The Human Rights Act 1998
- Environmental Information Regulations 2004
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Public Records Act 1958
- Re-use of Public Sector Information Regulations 2005
- Regulation of Investigatory Powers Act 2000 (RIPA)

Other related guidance and codes of good practice includes but is not limited to:

- Security Policy Framework (Cabinet Office)
- Public Service Network (PSN) Code of Connection
- Guidance and codes of practice published by the Information Commissioner's Office (ICO)

The Council is committed to high standards of data quality. We take every care to ensure that the data and information used throughout the organisation and in particular in performance management is **accurate, valid, reliable, timely, relevant, secure, accessible,** and **complete**.

2 Purpose

High-quality data is an integral part of the council's operational, performance management and governance arrangements so that it can drive service improvement and inform policy.

Our key objectives are:

- To ensure that service delivery is supported by good quality data.
- To ensure all staff understand and undertake their specific responsibilities in relation to data quality.
- To ensure that data produced, held and used within the council is of good quality.

- To enable effective, evidence based decision making supported by good quality data.
- To ensure that data quality is embedded across all services and is a key consideration for everyone dealing with data.

3 Scope

This policy document provides an overarching, corporate approach to the management of data quality. Service specific procedures will flow from this corporate policy, where relevant and necessary, ensuring that standards outlined in this policy are maintained throughout the Council.

This policy covers the quality of all data held by the Council only. This can be structured or unstructured. Structured data is based on a data model and is held in fixed fields in spreadsheets, databases and business systems. Unstructured data can be in any format including hand-written, textual documents or information gained from other sources.

Appendix 1 shows a list of the Council's key business systems where the key structured data for the Council is held.

The Policy is mainly aimed at officers and members of City of Lincoln Council but it applies equally to data used by the Council's strategic partnerships.

4 Policy

4.1 Governance, Roles and Responsibilities

This Policy applies to all staff within City of Lincoln Council as data quality is everyone's responsibility. However, where officers are assigned specific responsibilities in terms of data quality, these should be clearly defined and documented. The following table outlines the key roles and responsibilities for data quality:

Role	Responsibilities
Senior Information Risk Owner (SIRO)	To be the Council's champion for data quality with responsibility for formulation, implementation of policies and overall review and audit arrangements.
Data Protection Officer	To fulfil all duties as required under the GDPR (a statutory function)
Directors	Overall responsibility for the reliability of data and information presented to senior management and Members.
Assistant Directors	Responsible for ensuring: • that adequate, safe systems are in place which hold data of acceptable standard • that the data for their service is accurate, timely and meets relevant guidance • that actions arising from data quality audits are satisfactorily addressed • the implementation of corporate policy and procedures • training needs are identified
Internal Audit	Responsible for: • co-ordinating risk assessments of systems and audits in service areas where still applicable • ensuring improvements have been implemented • communicating and promoting commitment to Data Quality • providing training advice and guidance to services • regularly reviewing compliance with the data quality policy and liaising with appropriate officers to rectify non-compliance • Performance teams to carry out spot checks. • reporting on Data Quality issues to performance review meetings to DMT and CMT

Role	Responsibilities
Information Asset Owners (Service Managers and Team Leaders)	Responsible for: • knowledge of relevant data held within service areas • inputting accurate information on council systems • maintaining a robust control environment • identifying and rectifying gaps in control environment • providing information to their line managers/Head of Service and DMT as and when required
All employees	• Accurate and timely recording of data on appropriate systems • Adhering to the Councils Data Quality Policy

4.2 People and Skills

As an organisation we ensure that staff are in a position to undertake their responsibilities in relation to data quality. Training and development of staff and an understanding of the importance of data quality for Members underpin the achievement of high quality data and information. The following therefore has been considered across all service areas:

- Staff are made aware by their line manager of their responsibilities in relation to data quality.
- Staff have the relevant skills and competencies to fulfil their role in ensuring good quality data. They will receive appropriate training and guidance.
- Commitment to data quality is clearly communicated through the Council.

4.3 Systems and Processes

The Council ensures that appropriate systems are in place for the collection, recording, analysis and reporting of data. The Council recognises the importance of these systems operating on a right first time principle. Therefore, users are adequately trained and all systems have an appropriate training programme in place which is periodically evaluated and adapted as necessary.

The Council uses the principle of 'collect once and use numerous times' (COUNT) to underpin data collection and use.

4.4 Data Security

The Council ensures that data is stored in a secure environment with appropriate security and system backups for all business critical systems. The access and use of data should be appropriate to the data user and comply with relevant legislation including but not limited to, the legislation, guidance and codes of practice listed in

the Overview above and the Council's IT security policies. Systems are regularly tested to ensure that they are secure. The Council's Business Continuity Plan will make provisions for the business critical systems listed at Appendix 1.

4.5 Information Sharing

The Council will ensure that formal frameworks for data sharing with partners are in place. Data quality requirements will be applied to data used by the Council and shared externally, or which is provided by partner or third party organisations. These requirements will be in the form of Information Sharing Agreements, contracts or service level agreements which specify the responsibilities of partners to provide data which are fit for purpose. This includes complying with all legal, compliance and confidentiality standards.

The Council will have regard to the Transparency Board's Public Data Principles as set out in Appendix 2.

5 Policy Compliance

5.1 Compliance Measurement

The Council will ensure that it has effective validation processes in place to ensure the accuracy of data used in managing services and service performance. These will include:

- An ongoing programme of data quality audits undertaken by the Internal Audit service. The outcomes of these audits are reported to IT and Information Governance Board
- Reviews of systems and process undertaken by Internal Audit.
- The development and implementation of service specific Data Quality Assurance frameworks.
- Data returns are supported by clear and complete audit trails and subject to directorate and corporate verification checks.
- Any shortcomings identified during audits are corrected within agreed timescales.

Independent audits of data are reported to the IT and Information Governance Board. Improvement recommendations arising from internal and external audits are acted on so that there is continuous improvement to the Council's approach to data quality.

5.2 Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

5.3 Policy Review

This policy will be reviewed every two years and updated in the interim as required.

6 Related Standards, Policies, and Processes

The primary legislation governing the Council's information management activities is described in the Legal Responsibilities Policy.

7 Definitions

For the purposes of this policy the following definitions will be used:

- **Data**: Numbers, words or images that have yet to be organised or analysed to answer a specific question.
- **Information**: Produced through processing, manipulating and organising data to answer questions, adding to the knowledge of the receiver.
- **Knowledge**: What is known by a person or persons? This involves interpreting information received, adding relevance and context to clarify the insights the information contains.

The Council takes guidance from and uses the Audit Commission's "Standards for Better Data Quality". These are:

- **Accuracy** – data should be sufficiently accurate for their intended purposes.
- **Validity** – data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions.
- **Reliability** – data should reflect stable and consistent data collection processes across collection points and over time.
- **Timeliness** - data should be captured as quickly as possible after the event or activity and be available for the intended use quickly and frequently enough to support information needs and to influence service or management decisions.
- **Relevance** – data should be relevant to the purposes for which they are used. This entails periodic review of requirements to reflect changing needs.
- **Completeness** – Data requirements should be clearly specified based on the information needs of the organisation and data collection processes matched to these requirements.

Appendix 1 - The Council's Business Critical Systems

This Appendix lists systems used to create, process, and store data that are critical to the council's business.

Business System	Information Asset Owner (IAO)
Agresso Business World	Financial Services Manager
APP	Service Managers for each module
Autocad	Property Services Manager
Banking	Financial Services Manager
Benefit Debtors	Head of Shared Revenues and Benefits
BIDs Debtors	Head of Shared Revenues and Benefits
Building Control	Planning Manager
Cadcorp GIS	Business Development and IT Manager
CCTV	Community Services Manager
Choice Based Lettings	Housing Solutions Manager
Committee Management System	Legal and Democratic Services Manager
Contaminated Land	Environmental and Corporate Safety Manager
Council Mortgages	Head of Shared Revenues and Benefits
Council Tax	Head of Shared Revenues and Benefits
Electoral	Legal and Democratic Services Manager
Email	Business Development and IT Manager
EstatePro	Investment Manager
Gower – crematorium	City Services Manager
Housing Benefits	Head of Shared Revenues and Benefits
Housing Rents	Tenancy Services Manager
ICES Parking	City Services Team Leader
IMPS Performance Management	Principal Policy Officer
JONTEK	Housing Support Services Manager
LACHS	Financial Services Manager
Land Charges	Business Development and IT Manager
LloydsLink	Financial Services Manager
Metric Parking Office	City Services Team Leader
Midland Payroll	HR Manager
Mobile Device Management	Business Development and IT Manager
NNDR	Head of Shared Revenues and Benefits
P2.net	Property Services Manager
PCF Bacs	Financial Services Manager
Planning	Planning Manager
Repair Locator	Tenancy Services Manager
Repairs Scheduling	Maintenance Manager
Safety Organiser	Environmental and Corporate Safety Manager
Servitor	Maintenance Manager
Snap Survey	Principal Policy Officer
Universal Housing	Tenancy Services Manager
Voice Recording	Business Development and IT Manager
Website CMS	Business Development and IT Manager
WFM	Customer Services Manager

Appendix 2 - Transparency Board's Public Data Principles

(1) Public data policy and practice will be clearly driven by the public and businesses that want and use the data, including what data is released when and in what form

(2) Public data will be published in re-usable, machine-readable form

(3) Public data will be released under the same open licence which enables free re-use, including commercial re-use

(4) Public data will be available and easy to find through a single, easy-to use, online access point (www.data.gov.uk)

(5) Public data will be published using open standards, and following relevant recommendations of the World Wide Web Consortium (W3C)

(6) Public data from different departments about the same subject will be published in the same, standard formats and with the same definitions

(7) Public data underlying the Government's own websites will be published in re-usable form

(8) Public data will be timely and fine-grained – Data will be released as quickly as possible after its collection and in as fine a detail as is possible. Speed may mean that the first release may have inaccuracies; more accurate versions will be released when available.

(9) Release data quickly, and then work to make sure that it is available in open standard formats, including linked data forms – Linked data standards allow the most powerful and easiest re-use of data. However most existing internal public sector data is not in linked data form. Rather than delay any release of the data, our recommendation is to release it 'as is' as soon as possible, and then work to convert it to a better format.

(10) Public data will be freely available to use in any lawful way

(11) Public data will be available without application or registration, and without requiring details of the user

(12) Public bodies should actively encourage the re-use of their public data

(13) Public bodies should maintain and publish inventories of their data holdings

(14) Public bodies should publish relevant metadata about their datasets and this should be available through a single online access point; and they should publish supporting descriptions of the format provenance and meaning of the data

Source: https://data.gov.uk/sites/default/files/Public%20Data%20Principles_For%20Data.Gov%20%281%29_10.pdf

This page is intentionally blank.

Data Protection Breach Management Policy

Document Control

Organisation	City of Lincoln Council
Title	Data Protection Breach Management Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018- Executive
Filename	Data Protection Breach Management Policy
Version	V.4.1
Protective Marking	Not Protectively Marked
Next Review Date	July 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V 1.0	Becky Scott and Matt Smith	April 2014	Published version
V 2.0	Becky Scott	June 2015	Minor amendments
V 3.0	Becky Scott and Matt Smith	May 2016	Amending contacts list and implementing online reporting form.
V4.0	Gavin Thomas	May 2016	Minor changes post proof read
V 4.1	Becky Scott	June 2018	Updating policy in view of General Data Protection Registration (“GDPR”) and new Data Protection Act 2018 (“DPA”), and amendments to roles

Data Protection Breach Management Policy

Background

A data security breach can happen for a number of reasons:

• Loss or theft of data or equipment on which data is stored
• Inappropriate access controls allowing unauthorised use

• Equipment failure
Human error
• Unforeseen circumstances such as a fire or flood
• Hacking attack
• 'Blagging' offences where information is obtained by deceiving the organisation who holds it
• A deiberate act by someone disclosing data

Reason for the policy

The Council has to comply with legal framework for data protection to ensure that all data which is held is protected on behalf of all data-subjects. The Council also has a duty to protect all staff, members and the Council from legal challenge and subsequent cost implications and damage to the Council's reputation.

Time is of the essence

The Council encourages the notification of breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. This so that the Council can take immediate steps to recover the data if at all possible, and contain the breach.

Please telephone immediately when the breach/potential breach is noticed the Data Protection Officer or the Legal and Democratic Services Manager or if unavailable a member of the legal team to initially report the breach and provide brief details

Consequences of failing to comply with the DPA

It is recognised that data protection breaches may happen, and that the majority of times it will be human error which has caused the breach. However if individual staff members are found to be have failed to comply with the DPA, it could result in disciplinary action which could lead to dismissal. In addition, an individual can be criminally prosecuted under the DPA and/or liable to pay compensation in any civil action. Timely notification by an individual who thinks a breach has taken place will be taken into account in any resulting disciplinary investigation, as well as assistance in the containment of the breach.

Early reporting of data breaches is essential as under the General Data Protection Regulation which came into force on the 25th May 2018 and the DPA it is mandatory to report certain breaches to the ICO within 72 hours and also to data subjects in certain circumstances. These reports if required will only be made by the Data Protection Officer or Legal and Democratic

Services Manager or if both unavailable a member of the Legal team, after carefully consideration of the risks.

Policy contents

However the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery

2. Assessment of ongoing risk

3. Notification of breach

4. Evaluation and response

The policy must be considered to ensure that the Council deals with the breach appropriately and lawfully and there is an online form and a checklist to assist in this process.

Checklist for the Breach Management Policy

1	Contact the Data Protection Officer or Legal and Democratic Services Manager or if unavailable a member of the legal team immediately to report the potential breach	
2.	Contact any other relevant officers (see below) if required plus the relevant Director or Assistant Director and appoint a Lead Officer to investigate the breach.	
3	Complete a Containment and Recovery Plan to maximise the chances of recovering the data, and include procedures for damage limitation – complete the Data Breach Report Form see link below.	
4.	A Risk Assessment will then need to be completed by Data Protection Officer/Legal Services to assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, this is to include potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen	

5	Evaluation and response – it is important the causes of the breach are investigated by Data Protection Officer/Legal Services and that they also evaluate the effectiveness of your response to it and any potential learning points. A report from Audit may be required.	

Contacts

Data Protection Officer	Sally Brooks	Ext 3765	Responsible for data protection matters for the Council and therefore should be notified immediately of any data protection breach
Senior Information Risk Owner	TBC		
Legal Services Manager/ Freedom of Information Officer	Becky Scott	Ext 3441	Freedom of Information Officer
Chief Finance Officer	Jaclyn Gibson	Ext 3258	Responsible for financial matters
BDIT Manager	Matt Smith	Ext 3308	Responsible for all IT security
Audit Manager/Deputy	John Scott/Paul Berry	Ext 3321/3836	Needs to be made aware of any breaches to prepare report
Communications Manager	Steve Welsby	Ext 3318	To be kept up to date on the breach and the actions to be taken
Information Commissioner's Office	0303 123 1113 or 01625 545745		To be informed if a serious breach has occurred, in conjunction with the DPO/Legal Services.

Further information

Legal Services team

To access the Information Commissioner's Office website, click here

To access the Data Breach Report Form, click here

To access the ICO's guidance on Data security breach management, click here

Freedom of Information Act and Environmental Information Regulations Policy

Document control

Organisation	**City of Lincoln Council**
Title	**Freedom of Information Act and Environmental Information Regulations Policy**
Author - name and title	**Becky Scott, Legal and Democratic Services Manager**
Owner - name and title	**Becky Scott, Legal and Democratic Services Manager**
Date	July 2018
Approvals	**July 2018 Executive**
Filename	**FOI Policy**
Version	**V 1.1**
Protective Marking	**Official**
Next review date	**July 2020**

Document Amendment history

Revision	Originator of change	Date of change	Change description
V1.1	**Becky Scott LDSM**	**June 2018**	Updating policy in view of General Data Protection Registration ("GDPR") and new Data Protection Act 2018 ("the Act"), and amendments to roles

Contents

Overview

City of Lincoln Council (the Council) takes its responsibilities for the management of the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) seriously.

This Policy addresses risks associated with failing to comply with relevant legislation and outlines our approach to responding to requests for information made under the FOIA and the EIR.

It provides a framework to make sure that we fully support and consistently apply the principles of Freedom of Information, and meet the standards set out in the Lord Chancellor's Code of Practice on satisfying public authorities' obligations under the FOIA and the EIR.

The Policy aims to promote greater openness and to build public trust by providing access to information. We believe that access to information about decisions we take can help local people to influence local service provision. This will be balanced against the need to protect the confidentiality of, for instance, personal and commercially sensitive information.

1 Purpose

The purpose for having this Policy is to ensure that the Council foster a culture of openness and honesty in everything we do. By providing ready access to information we aim to build public trust and help local people to influence our decisions and improve our services.

2 Scope

This Policy applies to all employees, elected members, contractors, volunteers, agents and representatives and temporary staff working for the Council.

This Policy does not cover requests for access to personal information. These are exempt from the FOIA under section 40 and are processed in line with the Data Protection Act 2018.

3 Policy

3.1 Responsibilities

- The Council recognises there is corporate responsibility to give the public a general right of access to all information held by the Council.
- The senior officer with overall responsibility for the Council's compliance with legislation, and therefore this policy, is the Chief Executive. The implementation of, and compliance with, this Policy is delegated to the Senior Information Risk Owner (SIRO).
- Directors are responsible for promoting openness and accountability in their directorates.
- The Data Protection Officer's role is defined by the GDPR and is a statutory role

- The Legal and Democratic Services Manager, as the nominated FOI Officer, is responsible for drawing up guidance on freedom of information and promoting compliance with this policy to allow easy, appropriate and timely retrieval of information.

- The FOI Officer is also responsible for monitoring and reporting to the members of the Information Governance Board (AD Group) and Audit Committee on responses to requests for information.

- The FOI Officer will also provide an advisory service to the remainder of the Council.

- Information Asset Owners must make sure that all staff are aware of the requirements of the legislation and that all new staff receive an induction briefing on the access to information procedures.

- All staff must recognise that all recorded information may be given to the public and that in every case the law requires that there will be full and unconditional disclosure unless one of the legal exemptions/exceptions applies.

3.2 Available guidance

Guidance on the procedures necessary to comply with this Policy is available for Council staff from the FOI Officer and on the Council's Intranet, City People.

3.3 The Council's Publication Scheme

The Council is required by FOIA to maintain a Publication Scheme and to review this regularly. This is available on the Council's website or on request.

The Publication Scheme specifies:

- what information the Council will make routinely available to the public;

- how it will do so; and

- if information will be made available free of charge or on payment of a fee.

3.4 Specific requests for information

Information not already made available in the Council's Publication Scheme is accessible through a specific request for information. In this regard the FOIA establishes two related rights:

- the right to be told whether information exists; and

- the right to receive the information (subject to exemptions).

The EIR provide public access to environmental information held by public authorities.

The Regulations do this in two ways:

- public authorities must make environmental information available proactively;

- members of the public are entitled to request environmental information from public authorities (subject to exceptions).

The rights under FOIA and EIR can be exercised by anyone worldwide. Requests for access to information not listed in the Publication Scheme will be processed through this Policy and the Council's Data Protection Policy.

Requestors will be entitled to all the information unless one of the legal exemptions/ exceptions applies. However, only those specific pieces of information to which the exemption/exception applies will be withheld.

Where the Council has decided that an exemption/exception applies it will, if appropriate, consider the prejudice test and/or the public interest test and may in some circumstances withhold the requested information.

The Council is required by FOIA and EIR to respond to all requests within 20 working days although further reasonable details can be requested to identify and find the information in line with the legislation. If a fee is required, the Council will issue a fees notice and the applicant has 3 months in which to pay before their request is considered as being withdrawn.

3.5 Charges

Unless otherwise specified information made available through the Council's Publication Scheme will be free of charge.

The Council reserves the right to charge a fee for dealing with a specific request for information not listed in the publication scheme in line with the legislation.

3.6 Re-use of Public Sector Information

The Re-use of Public Sector Information Regulations 2015 (RPSI) are based on the principles of fairness and transparency and require that information is available for re-use unless exempt. They also state how the Council should respond to a request for the re-use of information.

RPSI includes all information whatever its content or format, where the Council holds the copyright and either produces, holds or disseminates the information as part of the Council's public task.

RPSI is about permitting the re-use of information not accessing the information. All requests for access to information which are unpublished by the Council will be dealt in line the Council's Data Protection Policy if personal information or this Policy.

The request for re-use must in writing, indicating the requester's name and address for correspondence, specifying the information requested and purpose for which they intend to use the information. The Council must then respond to the request in 20 working days although there are extensions available for volume and complexity in line with the legislation.

The Council will allow published information on the Council's website and Publication Scheme, unless otherwise specified, to be available under the Open Government License. This means that no specific request has to be made for the information and the information can be used freely. This is providing the re-user follows the terms of the License and includes an attribution statement in their products and applications where they include the Council's information.

In respect of unpublished information the Council may, where appropriate, apply charges, fees and restrictions to the information requested, in line with the legislation.

3.7 Datasets

The Protection of Freedoms Act 2012 added to FOIA duties in relation to providing datasets in response to requests and under a Publication Scheme. These provisions are contained in s11, 11A, 11B and 19 of FOIA.

The provisions state that where the Council is providing information which constitutes a dataset and the requester has expressed a preference to receive the information in electronic form, the Council must provide it in a re-usable form so far is reasonably practicable.

Re-usable means machine readable and based on open standards. Factors that can affect whether it is reasonably practicable are time, cost of conversion, technical issues and resources of the Council.

These provisions do not apply to information subject to EIR although the Council should note regulation 6 of EIR relating to the form or format of environmental information provided.

3.8 Complaints

An individual has the right to complain about the response they have received regarding their request for information. Details of the Council's Complaints Procedure are available for Council staff on request from the FOI Officer, on the Council's Intranet, City People and on the Council's website.

3.9 Compliance Measurement

The Council is required to maintain a public record for monitoring purposes of all FOI and EIR requests.

The Council will monitor and record the level and nature of requests and where requests are refused, the reasons for the refusal, including the exemption/exception used.

The monitoring results will be used by officers to decide what information can be included in the Council's Publication Scheme.

3.10 Non-Compliance

A deliberate or reckless breach of this Policy may result in a member of staff facing disciplinary action. Information Asset Owners must ensure that all staff familiarise themselves with the content of this policy.

The Council encourages the notification of breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. Notification will also be taken into account in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach.

Employees should also be aware that it is a criminal offence for individuals and/or the Council under s77 of FOIA to deliberately destroy, hide or alter requested information to prevent it being released.

Non-compliance of this Policy may result in an individual who is dissatisfied with the way their request for information has been handled, making a complaint through the Council's Complaints Procedure. If the requester remains dissatisfied then ultimately they have the right to make a report to the ICO.

The ICO is the body responsible for enforcement and arbitration under FOIA and EIR. The ICO through the Information Tribunal process has the authority to use the Courts to enforce its decision notices. Failure to comply with a decision notice is punishable by a fine.

A report to the ICO by a dissatisfied requester could therefore result in Council facing costly enforcement action, in addition to reputational damage.

3.11 Policy Review

This Policy will be reviewed every two years and updated in the interim as required.

4.0 Related Standards, Policies, and Processes

This policy relates to other Council Policies, in particular:

-Information Governance Policy

-The General Data Protection Regulation and Data Protection Policy

-Legal Responsibilities Policy

-Information Sharing Policy

-Data Quality Policy

-Data Protection Breach Management Policy

-Records Management Policy

-Information Security Policy

-Retention and Disposal Policy

5.0 Definitions

- Information	- *"Information is data imbued with meaning and purpose". Anon* - Information is something which tells us something and can also be communicated to someone else in a meaningful way. Information is data that is put into context, can be comprehended, understood and shared with other people and / or machines. - FOIA and EIR covers any recorded information held by public authorities, regardless of how it was created, received, stored or whether in paper, electronic format, email, microfiche or film.
- ICO (Information Commissioner's Office)	- The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. www.ico.org.uk
- Environmental Information	- Environment information includes for example, information about land development, pollution levels, energy production, and waste management. However the term is very broad and it is important to refer to the definition in regulation 2(1) before making a final decision as to whether the information is environmental.

- Personal information/data	- Article 4 of GDPR defines personal data as meaning *any information relating to an identified or identifiable natural person ('the Data Subject'). An identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier'* - The GDPR has expanded the definition of personal data to reflect changes in technology and includes online identifies such as an IP address and location data where they directly or indirectly identify individuals. Data which has been Pseudonymised (key coded) can also fall within the definition of personal data depending on how difficult it is to attribute the pseudonym to a particular individual. - Personal information is exempt from FOIA and EIR and a request for such information should be processed in line with the Council's GDPR and Data Protection Policy.
- Information Asset Owner	- The IAO was established by the Security Policy Framework and the role is included in the Information Governance Strategy. Their role is to protect and manage information held in the Council, and ensure that its value to the organisation is recognised. They are also responsible for promoting and fostering a culture of security of data within their teams and wider organisations - Information Asset Owners within the Council are all Service Managers and where appropriate Team Leaders.

- Absolute Exemptions under FOIA	- Absolute exemptions are where the information does not need to be provided. There is no need to apply any Public Interest Test as harm to the public has already been established. - Absolute exemptions are included in Part II of FOIA and can be applied where; • the information is already reasonably accessible by other means • information supplied or relating to security matters (not likely to be used by the Council) • court records (legal proceedings) • parliamentary privilege (only applies to central government) • personal information • information provided in confidence (provided from outside of Council and to disclose would lead to breach of confidence actionable in Court) • disclosure prohibited by any other legislation

- Qualified Exemptions under FOIA	- These exemptions are not absolute and are subject to the 'Public Interest Test' i.e. is the public interest in withholding the information and therefore applying the exemption greater than the interest in disclosing the information. - If the answer to the test is yes, then the information need not be provided if one or more of the Qualified Exemptions apply. These are also detailed in Part II of FOIA and can be applied where; • the information is intended for future publication • national security (unlikely to be used by the Council) • investigations and proceedings by public authorities • formulation of government policy • prejudice to effective conduct of public affairs • communications with Her Majesty • information that if released would endanger the safety, physical mental health of an individual. • environmental information • legal professional privilege - There are further Qualified Exemptions detailed at Part II of FOIA where a further test is to be applied following the Public Interest Test being the 'Prejudice Test' i.e. would the release of the information cause prejudice to individuals or processes. - If the answer to both tests is yes then the information need not be provided if one or more of the relevant Qualified Exemptions apply. These are also included in Part II of FOIA and can be applied where; • information relates to defence (not relevant to Council) • would cause prejudice to international relations

	• would cause prejudice to relations between central government and devolved assemblies • would prejudice the economic interest of the UK or part of it and the financial interest of the UK government or any administration within the UK. • would prejudice an investigation or legal proceedings • a statutory audit of another public authority (only applies up to publication of the final report and not to internal audits) • information containing third party personal information covered by the Data Protection Act • information constituting a trade secret or disclosure would prejudice the commercial interest of any person, including the Council.

Exceptions under EIR	- These are included in Regulations 12 and 13 of EIR. They are all subject to the 'Public Interest Test'. These include; • not holding the information at the time of the request • request is manifestly unreasonable • request too general and have provided advice already • information is in draft or unfinished • information is an internal communication - To rely on the following exceptions the disclosure would need to adversely affect those listed below, although these particular exceptions cannot be used if the information is on emissions. • international relations, defence, national security and public safety • course of justice, fair trial, public authority to conduct criminal or disciplinary enquiry • intellectual property rights • commercial confidentiality provided by law • interests of a person who provided the information where not obliged to provide • protection of environment • personal data.
- Datasets	- A dataset is collection of factual, raw data (neither the product of analysis or interpretation, nor an official statistic which has not been materially altered) that the Council gather as part of providing services and delivering functions as a public authority, and that the Council hold in electronic form.

Records Management Policy

Document Control

Organisation	City of Lincoln Council
Title	Information Sharing Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018 - Executive
Filename	Records Management Policy
Version	V.1.1
Protective Marking	Not Protectively Marked
Next Review Date	July 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V 1.1	Becky Scott LDSM	June 2018	Updating policy in view of General Data Protection Registration ("GDPR") and new Data Protection Act 2018 ("the Act"), and amendments to roles

1. Contents

2. Overview

2.1. What is Records Management?

Records management is the practice of maintaining records from the time they are created through to their eventual disposal. This may include the classifying, storing, securing and destruction (or in some cases, archival preservation) of records.

Records management is about controlling records within a comprehensive regime made up of policies, procedures, systems, processes and behaviours. Together they make sure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the Council benefits from effective management of one of its key assets, its records.

Section 46 of the Freedom of Information Act 2000 (Code of Practice on Records Management) ("the Code") defines a record as:

"Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".

Records can be in any format. As the Code says:

"The code applies to all records irrespective of the technology used to create and store them or the type of information they contain. It includes, therefore, not only paper files series and digital records management systems but also business and information systems (for example case management, finance, and geographical information systems) and the contents of websites."

2.2. What records does the Council keep?

At City of Lincoln Council ("the Council"), we keep records about the way in which we carry out our statutory and other functions, the people to whom we provide services and others with whom we deal, our policies, procedures and decisions about everything that matters to us and that staff need to do their jobs. Our staff keep these records as part of their daily work.

2.3. The relevant legislation

When developing policies, procedures and guidance involving the management of records the Council will comply with the following legislation, regulations and guidance and any other legislation as appropriate:

- Data Protection Act 2018
- The Freedom of Information Act 2000
- Section 46 of The Freedom of Information Act 2000 (Code of Practice on Records Management)
- Re-use of Public Sector Information Regulations 2015
- Financial Regulations

- Employment legislation
- Health and safety legislation

3. Purpose

The Council is committed to improve the way in which it creates, maintains, uses and destroys information and records. The purpose of this Policy is to set out the framework of rules and principles we will put in place to achieve this.

4. Scope

Development of records management procedures and practices are the responsibility of the Senior Information Risk Owner (SIRO), Data Protection Officer and the Freedom of Information Officer/the Legal and Democratic Services Manager.
.

All employees and Elected Members are responsible for the records they hold on behalf of the Council. They must follow this policy and all procedures, guidance, including the Retention and Disposal Policy.

All records created by Council employees and Elected Members will remain the property of the Council.

The creation, maintenance and destruction of records are the responsibility of the department providing the service. Each department must manage records in accordance with this Policy and all associated policies and procedures. It is essential records are stored securely and the Asset Register is updated, so that the location of files are known by staff at all times Policy

We will make sure the following rules and principles are embedded in all our service provision and processes:

- We will manage records in appropriate management systems and organise them accordingly (for example alphabetically, numerically, in date order, etc). Where appropriate, reference numbers and/or version control will be applied to help with locating records in the future, and for identifying records stored prior to destruction.

- We will maintain the Retention and Disposal Policy to make sure that records are kept for a period defined by relevant legislation and regulations before they are destroyed.

- We will provide mandatory training for employees on the importance of managing records effectively. Elected members will also be trained.

- We will make sure that policies, procedure and guidance are used in conjunction with the Council's the Retention and Disposal Policy.

- Audits will be carried out to monitor compliance with policy, procedure and guidance for safe and legal management of records.

4.1. Accuracy of personal records and data

The Council will make sure that all information is processed in accordance with the DPA. The Council's Data Protection Policy explains how employees are expected to comply with the Act when creating and maintaining records on behalf of the Council.

All records must be accurate, up to date and not excessive. Any corrections, amendments or additions to a record are to be made in accordance with departmental procedures and a record of changes retained for audit purposes.

4.2. Access to records (Statutory public access)

Subject Access Requests

The DPA gives individuals the right to access their personal information held by the Council. Policy, procedure and guidance can be found in the Council's Data Protection Policy and related staff guidance. This can be found on the Council's intranet.

Freedom of Information

The Freedom of Information Act gives the people a right to know what decisions are taken on their behalf by the Council on how services are run. The Council has published a Publication Scheme which shows what information can already be accessed. Any information which is not detailed in the Publication Scheme can be requested under the Freedom of Information Act although there may be exceptions to this where statutory exemptions apply.

Further guidance and contact information can be found in the Council's Freedom of Information and Environmental Information Regulations Policy and related staff guidance. This can be found on the Council's intranet.

Environmental Information Regulations

The Government has issued regulations to local Government which make it easy for people to access information about the state of the elements of the environment (air, atmosphere, water, soil, landscape, natural sites and ecology, biological diversity, and genetically modified organisms). Some information related to this is contained within the Council's Publication Scheme.

Further guidance and contact information can be found in the Council's Freedom of Information and Environmental Information Regulations Policy and related staff guidance. This can be found on the Council's intranet Standards for the storage of paper records

The Council will make sure records are protected from damaging elements such as water, light, temperature, humidity, fire and infestation.

The security of the information will also be protected by keeping storage units and rooms locked when not in use, where possible. Access to keys will be restricted to the responsible service area employees.

4.3. Standards for managing electronic records and email

Records will be managed in line with the Council's Retention and Disposal Policy and destruction and offsite storage Procedures which can be found on the Council's intranet.

Regular housekeeping is essential to make sure stored records are kept for the appropriate length of time in line with retention and disposal schedules. Records which form part of a service must be saved into the relevant system or shared work areas.

The Information Security Policy has further information on appropriate management of electronic records and email and is available on the Council's intranet or on request from from the Freedom of Information Officer/the Legal and Democratic Services Manager.

4.4. Retention and Disposal Policy

The Council's Retention and Disposal Policy dentify the types of records held and length of time each document or electronic record must be retained, and when it should be destroyed. In some cases records are retained permanently.

Directorates are consulted on the types of records they hold and the appropriate length of time set for retention of those records are agreed. Requests can be made to change retention periods but there must be a valid business reason and agreement from the Data Protection Officer or the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team. Some retention periods are governed by statutory legislation so it is important retention periods are applied correctly when deciding how long to keep or destroy a record.

All records have different retention periods, for example the destruction date may be from last involvement (closed record/last action entry) or from date of birth. This must be checked on the corporate retention and disposal schedules.

The Retention and Disposal Policy can be found on the Council's intranet Offsite Storage Procedure and Guidance

The Council is required to keep records for specified periods of time after involvements have ended. The length of time for keeping closed records varies dependent upon the nature of the involvement the Council had with the customer.

The retention period for each type of record is specified in the Council's Retention and Disposal Policy.

The Offsite storage procedure and guidance contains guidance in relation to the processes for preparing records prior to sending offsite and for retrieving closed records.

4.5. Corporate Records Destruction Procedure

The Council has a statutory duty under the DPA to make sure records relating to living individuals are not kept for an excessive amount of time. Where records exceed the retention period these must be destroyed unless there is a valid and legal reason for retaining.

If the responsible Directorate/department has a business need to retain information after the destruction date set, the Data Protection Officer or Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team must be notified and an agreement reached to change. Policy Compliance

4.6. Compliance Measurement

The Council will ensure compliance with this Policy by regularly reviewing organisational and technological processes to ensure compliance with Section 46 of the Freedom of Information Act 2000 (Code of Practice on Records Management) and all other relevant legislation including the DPA.

Where there are particular compliance measurements required by the DPA and the Freedom of Information Act 2000 and Environmental Information Regulations 2004 these are detailed in the Council's relevant Policies.

All policies relating to Records Management will be subject to scrutiny by the Policy Scruntiny Committee and/or the Audit Committee.

4.7. Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in prosecution, financial loss and damage to Council's reputation and ability to provide necessary services to our customers.

If any user is found to have breached this Policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

The Council encourages the notification of Data Protection breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. Notification will also be taken into account in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach.

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the Data Protection Officer and the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team.

4.8. Policy Review

This Policy will be reviewed every two years and updated in the interim as required.

5. Related Standards, Policies, and Processes

- Information Governance Policy
- Legal Responsibilities Policy
- Information Sharing Policy
- Data Quality Policy
- Data Protection Breach Management Policy
- Freedom of Information Policy & Environmental Information Regulations Policy
- Data Protection Policy
- Information Security Policy
- Retention and Disposal Policy

6. Definitions

Asset Register	The detailed breakdown of all records and information held by the Council and signed off by the Information Asset Owner. This includes details of location, format, security access restrictions, data flows and asseses any risks to assets.
Records management	The discipline and professional function of managing records in order to meet organisational needs, business efficiency and legal and financial accountability.
Information Asset Owner	The IAO was established by the Security Policy Framework. Their role is to protect and manage information held in the Council, and ensure that its value to the organisation is recognised. They are also responsible for promoting and fostering a culture of security of data within their teams and wider organisations. Information Asset Owners within the Council are all Service Managers and where appropriate Team Leaders.

SIRO	Senior Information Risk Owner. Leads the organisation's reponse on information risk and is responsible for ensuring organisation's information is managed securely. They are often a senior individual within the organisation and are a main point of contact for IAO's.
Retention	Means the length of time for which records are to be kept. Thus it normally represents and will be expressed as a disposal period.
Disposal	In this context does not just mean destruction: it embraces any action taken (or yet to be taken) to determine the fate of records including transfer to a permanent archive.
Information security	The policies, procedures and practices required to maintain and provide assurance of the confidentiality, integrity and availability of information.
Compliance	In the context of Information Management, compliance relates to the Council's need to operate in accordance with the existing legislation, regulations and best practices.

Date: July 2018

Subject: Record Retention and Disposal Guidelines

1. Introduction

- Council records and the information they contain have a high operational and functional value and are regarded as Information Assets within the Information Management environment. In the same way that the Council will seek to protect and manage its physical assets, Information Assets should be effectively managed, lawfully exploited and adequately protected.

- One aspect of good practice in records management is controlling the retention and disposal of records so that operational, legal and regulatory requirements are appropriately met.

In respect of personal data (identifying living individuals) the Data Protection Act 2018 states that such information shall not be kept for longer than necessary in a form that permits identification of the data subject. Breaching this may result in substantial fines and reputational damage to the Council.

2. What should I be aware of?

Record Retention and Disposal Guidelines

- The Council already has in place documented ***Record Retention and Disposal Schedules*** that can be accessed on the Council's intranet and website. The objectives of the guidelines are to:
    - Assist in identifying records that may be worth preserving permanently as part of the Council's archives;
    - Prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration;
    - Provide consistency for the destruction of those records not required permanently after specified periods; and
    - Promote good records management practice.

- The guidelines are structured around types of records and define the periods for which the records must be retained in order to comply with legislation and regulations. The contents are structured on formats defined by the Local Government Association.

- Information Asset Owners (managers/team leaders) must be aware of the defined retention periods for the records maintained within their operational areas and ensure their compliance. The Council could be penalised, incur additional costs and face disruptions if records were to be disposed of prematurely or kept beyond their retention period.

Legal and Regulatory Implications

- The Council must comply with a range of statutory, regulatory and financial requirements in relation to the maintenance and retention of records (for example, the Public Records Act 1958 and the prevailing HMRC VAT regulations).

  The Data Protection Act 2018 places additional obligations on the Council with respect to retaining and disposing of records in order to protect personal information and the rights of data subjects.

Disposal and Destruction of Records

- Records must only be disposed of or destroyed in strict accordance with the periods defined within the Record Retention and Disposal Schedules and the requirements of the Council's Records Management Policy. Records earmarked for permanent preservation should only be deposited in an appropriate and secure Council archive facility or official local or national archive.

- The physical destruction of records must be undertaken in a secure manner by approved contractors or staff operating in a secure facility that protects the records from loss and unauthorised disclosure.

- The disposal method applied should render the records unusable and unreadable (for example, cross-cut shredding).

- Unwanted hard drives that have contained Council records must be irreversibly destroyed and rendered unusable by the IT Section.

3. Required Actions

- Information Asset Owner's (IAO's) and staff should consider the range and type of records they create, maintain and use, and ensure that retention periods prescribed for that type of record within the Schedules are being complied with.

- IAO's should consider whether they have in place sufficiently robust measures to prevent the premature or inappropriate destruction of their records.

- Any possible instances of non-compliance should be brought to the attention of the City Solicitor so that appropriate action can be taken.

- IAO's should consider how they currently dispose of records that are no longer required and whether the methods employed are adequately secure.

4. Sources of Further Information

- The Council's ***Record Retention and Disposal Schedules*** (available from the Council's intranet and website)

- All staff should become familiar, with the following documents and their responsibilities:

- GDPR and Data Protection Policy
- GDPR and Data Protection Policy Summary Sheet
- Freedom of Information Policy Summary Sheet

- Staff should initially seek clarification from IAO's (their line manager or team leader).

- Any remaining specific queries should be routed as follows:

    - Data Protection Officer- Sally Brooks-Ext 3765.

    - Freedom of Information Officer – Becky Scott (Legal & Democratic Services Manager – Ext 3441).

    - Security and use of IT records – Matt Smith (Business Development and IT Manager – Ext 3308).

This page is intentionally blank.

AUDIT COMMITTEE **19 JULY 2018**

SUBJECT:	**INFORMATION MANAGEMENT UPDATE**
DIRECTORATE:	**CHIEF EXECUTIVE AND TOWN CLERK**
REPORT AUTHOR:	**DATA PROTECTION OFFICER**

1. Purpose of Report

1.1 To update Audit Committee on the progress of the information management project and the implementation of the EU General Data Protection Regulation (GDPR).

2 GDPR Action Plan Progress

2.1 The GDPR Action Plan is attached at Appendix A.

2.2 The GDPR Group have been prioritising becoming compliant and completing the project prior to the GDPR coming into force on the 25 May 18. There is however a lot of work still to be done and ongoing actions, particularly in the following areas:-

(a) Training

Action:

Ongoing Data Protection training (Article 32 GDPR-testing effectiveness of organisational measures for security of processing) and ensure renewed every 2 years and non-completion followed up. Include member training. Implement ongoing training needs plan.

There is a need to finalise the initial DP training however the ongoing training will be essential and needs to be programmed as to how this will be achieved, and will be made easier now Netconsent is in place. Initial training figures are approximately at 90% completion for all staff and rising. Given these figures include recent leavers and those on long term leave it is unlikely that 100% will be achievable.

(b) Privacy Impact Assessments

Action:

Data protection Privacy Impact Assessments- Article 35 of GDPR Introduces a formal Policy to require a DPIA. Conduct a DPIA for new systems that involve the processing of personal data, or significant changes to existing systems. Such DPIA's should be signed off at an appropriate level and implemented into project planning at the earliest stage.

A DPIA process in now in place and has been integrated into the project management model. Various teams have completed these in respect of assessing how we process personal data before a project/piece of work, for example, a new IT system for Housing Solutions and processes for Universal Credit Support and Assistance.

In addition since GDPR came into force in May 18 these assessments are mandatory in particular circumstances including retrospectively for core systems processing large amounts of sensitive data. Assessments for existing systems are being undertaken in an applications review by Audit team with system owners.

(c) Contract review for GDPR clauses

Action:

Contracts with Processors Article 28 identify contracts for review and ensure these and new contracts are GDPR proof. Joined up approach with Legal and Procurement

Each contract for CLC which includes personal data needs to be reviewed and amended to comply with the GDPR. The DPO and the LDSM are finalising the standard clauses to be used and aim to contact all suppliers on behalf of contract managers and to vary the contracts. It is vital that we ensure that the contracts register is up to date so that we can ensure that all contracts are captured.

IAO's have been declaring all contracts and populating them into our contracts system along with the partnership register. This process is being overseen and signed off by AD's. The DPO and LDSM have also been responding to supplier's who have contacted CLC with their own contract variations. Given the volume of contracts this will be a long process.

(d) Record of Processing Activities

Action:

Record of Processing Activities (ROPA) - Article 30 to be prepared based on the asset register to include data sharing details and legal basis for processing. ROPA database to be designed and implemented

We have an asset register complied by the DPO after extensive work with IAO's. This needs to be kept up to date by IAO's and this needs to include the legal basis for processing. The register does include a description of information being shared although this may need to be expanded upon in some areas. An IAO annual checklist for data protection will be issued shortly which includes their agreement to maintain their part of the register and continue to assess their information assets.

(e) Individual Rights

Action:-

Rectification, right to be forgotten, data portability- Articles 16-20. Document the review and weeding process for software systems storing personal data. This task should have an assigned owner and be monitored. Develop plan for 'weeding' of data as part of R&D work.

The BDIT Manager continues to work on this area however solutions are complex, and options potentially expensive and resource intensive. IAO's should encourage their teams to review the information they hold in 'drives' and mailboxes and delete any unnecessary information. BDIT have been actively contacting IAO's to assist with implementation in IT systems and progress is being made.

(f) Policies and procedures

Action:

Draft a GDPR policies to be implemented and agreed before May 2018 to replace Data Protection Policy and Summary sheet. Obtain approval and issue to staff.

A GDPR and DP policy was issued to all staff via Netconsent prior to the 25 May 18 which they were required to read and accept. All information management policies were reviewed in May 18 and following approval will be rolled out to staff.

The above actions are the ones which the IG/GDPR group would highlight as being the more complex ongoing actions where extensive resources are needed, particularly for the DPO and also time from all other staff involved to ensure we can achieve compliance.

3 AGS

3.1 The AGS status for the Information Governance section is now amber, and all the work being undertaken for the implementation of the GDPR will be reviewed in due course to see whether the Council might improve this status.

4 Vision 2020

4.1 The GDPR project is one of the Vision 2020 projects to be delivered in year 2018/19. The Working Group was meeting monthly prior to the 25th May 2018 to ensure that we were on target with our Project Plan for the implementation of GDPR. The DPO and IG Group continues to implement the Plan.

4.2 This work ensures that staff are high performing in their collection and processing of customer's data. It also assists to ensure that the Council is trusted to deliver the services, and ensures compliance.

5 Organisational Impacts

5.1 Finance

Nothing relevant to this report.

5.2 Legal Implications

As outlined in the report.

6 Recommendation

6.1 To note the report and provide comments on the action plan

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	1
List of Background Papers:	None
Lead Officer:	Sally Brooks, Data Protection Officer Telephone (01522) 873765

General Data Protection Regulation (GDPR) Action Plan

V 0.6	Key
	Outstanding- failure attracts higher level fines- 20 million Euros
	Completed
	Outstanding-failure attracts lower level fine -10 million Euros

Ref	Action	Agreed action	At Dec 17 Work completed to date	At Jan 18 Work completed to date	At Mar 18 Work completed to date	At April 18	At May 18	At June 18	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
	Issues under ICO's 12 Steps to take now												
	1. Awareness												
1.1 Y	**Training**	Ongoing Data Protection training (Article 32 GDPR-testing effectiveness of organisational measures for security of processing) and ensure renewed every 2 years and non completion followed up. Include member training. Implement ongoing training needs plan.	All teams, IAO's and members training completed. Developed in house interactive e-learning package now up to 70% completion rate for all staff and rising. Need to continue to implement and monitor training needs plan.	Completion rate to be reviewed again at the end of Jan 18 and issued to AD's after recent issuing of low risk dp training sheet for staff with no or very little contact with personal data.	Completion rate to be reviewed again at the middle of March 18 and issued to AD's . GDPR specific training via video/e learning/Netconsent to go to IAO/s SM's early from May	E-learning % overall – 79.4% – 132 to complete % main – 85.5% - 84 to complete % low risk – 23.8% - 48 to complete. Member training booked in and training for apprentices (May 18) Briefing note on GDPR prepared for Cllrs to be issued May 18.	80.8% - 87% non-low risk, 23.8% low risk forms as at 14 May. AD's have since chased staff through Managers and informed of leavers and long term absences still on the staff list. So completion rates are better than they look and these staff can be removed on the next report. Mainly staff identified as being low risk need to complete and the relevant managers have been chased again.	As at the 19 June 18 90.5% overall completion – 64 not completed 91.9% higher risk – 50 not completed 77.8% low risk – 14 not completed	Completed but ongoing	Jul-18	List of staff not having completed the e-learning went to AD Group in Feb, March, April, May and June 18. The % includes staff on long term leave, maternity etc so % would be higher. Issued basic training sign off sheet for staff with limited or no access to personal data or PC	Need as near to 100% as possible. May not be achievable given starters leavers and long term absences.	DPO/LDSM/BDITM
1.2 G	**Comms**	Re-brand Data Protection (Article 32) Comms to use 'customer privacy' 'data privacy '. Re brand GDPR as Let's Get Data Privacy Ready. Raise awareness with GDPR Comms Plan.	Ongoing data protectors forum updates and Comms articles referring to GDPR. Have been posting now for over 1 year and records of these on Council's intranet city people. Have revised GDPR Comms plan moving towards 25 May 2018 (date GDPR in force)- 6 month plan.	Comms article issued late Dec17-clear up on emails retained. Jan 18 article regarding all emails being potentially disclosable on Dp forum. GDPR visual introduction to be issued by Comms end of Jan 18.	Jan 18 article regarding all emails being potentially disclosable on Dp forum. GDPR visual introduction issued by Comms in Feb. Article on mandatory data breach reporting issued in March	Comms going to week commencing 30 April re rights and sending general privacy notice out by net-consent to all staff for awareness same week	Comms Plan to be extended post 25 May 18.	Comms continues to be issued as and when required.	Completed but ongoing. Long term plan forms part of Vision 2020.	Jul-18		Pre GDPR Plan complete . Post Plan to be agreed	DPO/COMMS
1.3	**Policies, Guidance and procedures**	Draft GPDR Handbook for IAO's. Draft GDPR policies to be implemented and agreed before May 2018 to replace Data Protection Policy and Summary sheet. Obtain approval and issue to staff.	All information management polices were reviewed and approved in May 2016. All polices available on City People. IAO's should actively monitor compliance with the Policies in their business areas. All policies are due for review and implementation by May 2018. GDPR Handbook drafted for IAO, issued to IAO's discussed in training and available on City People.	Ongoing	GDPR handbook circulated and checklist in draft has been issued. To be finalised with netconsent soon. GDPR policy drafted to PSC on 20 March 2018 and Exec on 26 March 2018	GDPR Policy to be issued to all staff and members via net-consent May 18. (test questions to be drafted to test understanding on policy)	GDPR Policy issued to all staff by net-consent with skip days to the 25 May. Summary sheet issued to managers for staff with no access to net-consent.	Reviewed and amended IM Policies due to go to Audit 19/07/18 and Exec 21/07/18 for approval. Will be reissued with Comms to staff and uploaded into netconsent.	Completed but ongoing	Jul-18	Handbook prepared and checklist being rolled out 24 January. Summary sheet to be drafted and issued to staff. Include data subject's enhanced rights and changes to SAR's.	Completed	IAO's DPO/LDSM/BDITM
1.4 G	**Regular item at team meetings**	Consider incorporating data privacy as a regular agenda item at team meetings. Agree level for Data Protection issues to be discussed e.g. DMT/SMTs	Several IAO's are already incorporating need to ensure in all teams.	Included in report to AD's Jan 18.	Has been recommended to all IAOs through training/checklist and then to AD's. SMTF have agreed to put it on their agenda.	Ongoing			Quarterly-ongoing for teams		Included in IAO's checklist issued Jan 18 and SM's reminded in Feb meeting	Completed	IAO's
	2. Information the council holds												
2.1	**Information asset audit**	IMPs system to be fully populated and reports into Performance DMT	Information asset audit completed by IGO with all IAO's. IMPS system now fully populated with summaries and IAO's contacted to follow up and implement asset audit recs. IAO's previously given summary reports with own recs to implement	Outstanding recs being monitored in performance DMT. IAO's be chased again regarding outstanding recs.	Outstanding recs being monitored in performance DMT. IAO's be chased again regarding outstanding recs.	IMPS to be updated by managers. Ads to chase or be copied in to Mangers being chased. Director of DCE requested update and DPO provided 30 April	Audit recs being chased by AD's and updated by IAO's.	Long term audit recs such as retention implementation in systems being chased through managers' AD's and CLT.	Audit completed long term recs to be followed up	Jul-18	All IAO's sent IMPs recs as reminder to summaries. Need to follow up IAO's who have not responded.	IGO following up recs with IAO's.	IAO's /DPO
2.2	**Information asset register/ records of processing (ROPA)**	Information assets registers should be updated, reviewed and risk assessed on a periodic basis by IAO's	Registers issued to all IAO's. Training provided to update as and when required and at least every 6 months. Needs to form part of IAO self assessment checklist. Any changes to registers need to provided to the IGO to update corporate register. Guidance in IAO GDPR Handbook.	Work being completed towards ROPA. Consolidating asset register and identifying legal basis for processing.	Work being completed towards ROPA. Consolidating asset register and identifying legal basis for processing. Included in IAO's checklist	LGA have now issued interactive ROPA tool. To be considered by DPO and BDIT Manager as option to build on Asset Register data. Forum meeting to discuss with local DPO's at WLDC on 2 May	Have general privacy statement and asset register. Need to build up records in asset register. Decide whether we are using the LGA ROPA tool	Need to build on existing asset register. Will be issuing IAO checklist in July 18 and annually thereafter including maintaing aset register and assessing risks to assets.	Reviewed by IAO's every 6 months and as and when required.	Jul-18	Legal basis for processing being added and links to retention schedules and Sharing Agreements	IGO and BDIT resolved to have the ROPA developed before May 18	IAO/BDIT/DPO

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date				Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
2.3	**Retention and disposal schedules**	Ensure future adherence to retention and disposal schedules. This includes emails. Retention schedules updated and available on council's intranet.	R & D schedules updated and available on city people. IAO's responsibility to ensure compliance in their service areas. Form part of IAO checklist. Guidance in IAO GDPR Handbook.	Complete.	Complete.	BDIT also contacting IAO's to assist with retention in systems			Implementation reviewed by IAO's every 6 months and as and when required	Jul-18	Responsibility with IAO's	Complete save for monitoring	IAO's
2.4	I**nformation sharing-with our data processors-(Contracts)**	Contracts with Processors Article 28 identify contracts for review and ensure these and new contracts are GDPR proof. Joined up approach with Legal and Procurement	Received terms and conditions from procurement Lincolnshire and need to review. IAO's to assist to identify in their areas contracts which may need to be reviewed or put into place. Guidance in IAO GDPR Handbook.	CCS issued standard terms and conditions for contracts involving processing of personal data in Jan 18. Plan to list contracts and contact parties to agree variations where required.	Plan in place to list contracts and contact parties to agree variations where required. IAO's requested to populate contracts register and complete declaration in Mar 18. AD's to declare. Next stage to identify personal data contracts and prioritise. Obtain contact details to vary contracts	Plan ongoing, also considering GDPR contracts now issued by supplier's.	AD's chasing small number of IAO's yet to complete. AD's signed off process and DPO and Legal have started to amend on risk basis and processors who have contacted us.	AD's chasing small number of IAO's yet to complete. AD's signed off process and DPO and Legal have started to amend on risk basis and processors who have contacted us.	Dec-18	Jul-18	Progress with contracts and partnership register being up to date and sign off by IAOs and then AD's by 23 march then, we'll be able to contact suppliers	ID contracts where personal data and non framework to then contact suppliers	DPO/LDSM/PO and IAO's
2.5 G	**Information sharing-with other data controllers who are not processing on our behalf (ISA's)**	Information Sharing Agreements should be reviewed and consolidated and a database held in Legal Services. All data shared with external bodies should be subject to an ISA	A database of existing ISA's has been created. IAO's to have responsibility to identify in their area where ISA's may be required and seek advice from IGO/LDSM to implement. Guidance in IAO GDPR Handbook.	New ISA's being implemented and being identified for issue from new DPIA process.	New ISA's being implemented and being identified for issue from new DPIA process.	Ongoing-intention long tem to have database in netconsent			Completed but ongoing	Jul-18	Complete and ongoing	Review dates in IAO checklists. Consider whether review dates can be monitored through Netconsent	DPO/LDSM and IAO's
2.6 G	**ICO fees**	£2900 for the organisation £40 for councillors	Pay in Aug. when registration is up	Ongoing	Ongoing	Complete and ongoing			Aug-18	Jul-18	Complete and ongoing on annual basis	complete in Aug.	LDSM
3	**3. Communicating privacy information**												
3.1 Y	**Privacy statements (also a Right to be informed)**	Information provided where personal data is collected- Article 13 GDPR. IAO's must identify and review Privacy Notices in their areas which require amendment to comply. Amendments to be made with assistance from IGO where required. Review Council's general privacy statement on website.	Responsibility for Privacy Notices in service areas allocated to IAO's training provided and guidance in IAO Handbook. IAO's to seek advice from IGO where required. IAO's have revised their Privacy statements in several areas. The Council's general statement has been reviewed by IAO's and is to be amended following approval.	Being amended as IAO's identify and approach IGO team for assistance.	Being amended as IAO's identify and approach IGO team for assistance.	General privacy notice for Council drafted and to be issued to staff prior to be uploaded on to website for 25 May 18.	Customer notice was consulted on with staff and due to go live on 25 May. Staff notice issued to all staff by HR. Service specific notices being completed by IAO's with assistance from DPO.		Completed by ongoing	Jul-18	Now included in IAO's checklist but ongoing	Completed but ongoing	IAO's DPO - LDSM
4	**4. Individual's rights**												
4.1 Y	**Rights**	Rectification, right to be forgotten, data portability- Articles 16-20. Document the review and weeding process for software systems storing personal data. This task should have an assigned owner and be monitored. Develop plan for 'weeding' of data as part of R&D work.	Few systems have procedures for removal of personal data currently. The BDIT Manager has liaised with IAO's and contacted all suppliers of core systems. The responses received are varied and need to be assessed and plan actioned.	Ongoing discussions with a number of suppliers APP, I Trent, Index making changes due to GDPR and offering products	Ongoing discussions with a number of suppliers APP, I Trent, Idox making changes due to GDPR and offering products. Outcome some products are offering free upgrades, some are offering enhancements for fee. Enhancements can be achieved currently although would save time and resources. Need to assess cost/benefit and demand	Supplier's are now coming up with solutions and provided patches and updates. In some cases enhancements for a cost where system can manually achieve.	Dealing with systems as part of contracts review.	Ongoing discussions with system providers.	Ongoing	Jul-18	Suppliers have been in contact regarding GDPR changes to systems. Uniform for Planning. Civica for APP. Civica for Universal Housing. Considering reports to teams re data being over x years old.	Ongoing BDIT	BDITM/IAO's
5	**5. Subject access requests (SAR)**												
5.1 Y	**Rights requests**	Rights of access by the data subject- Article 15. Ensure we can comply with the additional rights of data subjects created by GDPR including the right to have their personal data deleted. Draft GDPR policy to replace the Data Protection Policy to include access to information request changes effective from May 18.	Policy to be prepared and reviewed following clarification of derogations in Data Protection Bill, and Comms plan to include access by subjects to data	Ongoing	GDPR Policy drafted and to go to PS March 18	Need to update request form and information on website (mainly contained in general privacy notice)	Staff informed of rights changes in Policy, customer and staff privacy notices. New SAR form and process to go live from the 25 May 18.		Completed but ongoing	Jul-18	Comms plan includes changes to access to information requests. GDPR policy drafted and summary sheet to be issued to staff by May 2018.		LDSM/DPO
6	**6. Legal basis for processing personal data**												

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date				Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
6.1 Y	**Legal bases**	Record of Processing Activities (ROPA)- Article 30 to be prepared based on the asset register to include data sharing details and legal basis for processing. ROPA database to be designed and implemented	Information regarding data held and information flows have been collated in the information asset register. Investigations are being undertaken as to how to build on these records and display them. the intention is to produce a basic record of processing activities by May with a view to expanding on this in due course, to be a full scale database or extending the asset register to provide more detail	Being identified on asset register for ROPA.	Being identified on asset register for ROPA.	Being identified on asset register and in privacy notices. LGA's ROPA tool to be considered.	Detailing in privacy notices and in asset register	Detailing in privacy notices and in asset register	Ongoing	Jul-18	Ongoing	Database being developed or/and information to be added to asset register and/or ROPA statement	BDITM/DPO
7	**7. Consent**												
7.1 Y	Consent	Ensuring whether we have valid Consent (Articles 7-8) from customer's where required by reviewing how we seek, obtain and record consent and whether we need to make any changes to comply with GDPR.	IAO's to assist IG team to identify areas where we are relying on consent alone to process personal data and review with assistance if necessary whether this consent is valid. Changes have already been made to consent statements in some areas. Guidance issued to IAO's In Handbook and face to face training.	Consents being altered as IAO's identify and approach IG team if required for assistance.	Consents being altered as IAO's identify and approach IG team if required for assistance.	Consents being amended where idenified by IAO's in their area.			Completed but ongoing	Jul-18	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's
8	**8. Children**												
8.1 G	**Obtaining personal data directly from children**	Identify any areas where we be may obtaining personal details and relying on consent from children under 16 years due to changes. DP Bill has reduced this to 13 years.	IAO's to assist IG team to identify areas where relevant and ensuring we have systems in place to verify individuals age and to gather parental or guardian consent for the data processing activity.	Not identified applicable in any areas to date.	Not identified applicable in any areas to date.	Not identified applicable in any areas to date.			Completed but ongoing	Jul-18	Included in IAO's checklist	Complete - ongoing monitoring	IAO's
9	**9. Data breaches**												
9.1 G	**Data breaches**	Ensure DP Breach Management (Articles 33-34) policy up to date and internal breach reporting system compliant with GDPR timescales for reporting. Monitor through IG group and officers for lessons learnt and trends.	Development of internal e-form Breaches being reported to IG Group. Internal breach reporting system effective with GDPR time scales i.e. 72 hours to report to ICO.	Ongoing Policy and reporting process in place.	Ongoing Policy and reporting process in place.	Ongoing and reporting			Completed but ongoing	Jul-18	Comms Plan includes changes to breach reporting and time limits.	Data Protection Breach Management Policy to be slightly amended to include GDPR changes and new time limits.	DPO/LDSM/BDITM
10	**10. Data protection by design and data protection impact assessments (DPIA's)**												
10.1 G	**Data protection impact assessments**	Data protection Privacy Impact Assessments- Article 35 of GDPR Introduces a formal Policy to require a DPIA. Conduct a DPIA for new systems that involve the processing of personal data, or significant changes to existing systems. Such DPIA's should be signed off at an appropriate level and implemented into project planning at the earliest stage.	DPIA Guidance has been drafted along with templates and Comms. Needs to be implemented for new processes with maybe an e-form to assist - focus on those mandatory ones. Project management guidance to be amended Build DPIA into SPIT process (or replacement process) for new systems and training rolled out where required	New simplified process developed and issued to IAO's across directorates for projects for completion. IGO assisting when requested.	New simplified process developed and issued to IAO's across directorates for projects for completion. IGO assisting when requested.	Process in place and has now been incorpotated into project planning model by Policy team			Completed but ongoing	Jul-18	Rolled out guidance, training done, in IAO handbook and checklist. Ongoing	Complete-ongoing and monitoring.	LDSM/BDITM /DPO Project Managers
10.2	**Build privacy by design (DPIA's) into project planning**	Review of Lincoln Project Model and Project Management	LDSM to meet with Policy to discuss once governance arrangements for projects are agreed	Ongoing discussions	Ongoing discussions	Complete			Completed but ongoing	Jul-18	LPMM to be changed	Review of project model and incorporate DPIA process	LDSM

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date				Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
10.3	**Security of processes**	Security of Processing- Article 32 implement technical and organisational measures to ensure a level of security appropriate to the risk. Consider pseudonymisation capabilities where encryption not available. Ability to restore access to data in event of an incident and regular testing of effectiveness of measures.	ICT policies already in place including security and restoration of data following an incident. Need to raise awareness of risks and explore if pseudonymisation software is necessary. Internal Audit underway regarding security of applications.	Ongoing	Ongoing	Ongoing			Completed but ongoing	Jul-18	Audit is ongoing	Ongoing BDIT	BDITM
10.4	**Access to applications**	Access requests for new starters should be made by appointed staff members with the appropriate authority. Network access should be suspended when staff are absent from work for an extended period, for example; due to maternity leave. Any failure by HR to notify IT of staff leavers or long-term absence should be treated as a security incident and reported to the IGO. Access to systems and drives should be reviewed regularly and at least every 6 months.	ICT policies already in place covering access requests and removal. In addition to this regular access reviews now being carried out in areas processing sensitive data such as Benefits every 6 months. Applications audit currently being undertaken by Audit. Previous Asset Audit identified issues with Access in some systems and relevant recs to be followed up. Access reviews included in handbook issued to IAO's	Ongoing	Ongoing	Ongoing			Completed but ongoing	Jul-18	Checklist includes this	Relevant System's team BDIT and IAO's	IAO's/AuditM/ BDITM
10.5	**Testing of security measures**	Testing effectiveness of security measures- Article 32. Prepare a Checklist for IAO's to complete following training in January 17 to ensure . Devise annual self assessment checklist for IAO's. Internal audit of IG	Handbook issued as guidance to checklist. Checklist to be issued annually. Include an aspect of information management in the 2017-19 Audit Plan where it is identified as a key risk by the ICO. The council could include records management as a standard item on the internal audit plan to ensure regular DPA compliance checks are completed. Sample monitoring of customer service calls including customer identification and verification questions already taking place.	Ongoing	Ongoing	Ongoing			Audit planned 18/19. Checklist issued to IAO's annually	Jul-18	Ongoing	Internal Audit	IAO Audit
10.6 G	**Physical security and clear desk policy**	IAO's to be reminded to carry out periodic spot checks of business areas adherence to the clear desk policy including the locking away of sensitive personal data and use of confidential waste bins. Also minimising the amount of personal data taken offsite.	Included in handbook. Transporting data securely between locations is included in REMOVAL guidance on city people. This was issued to staff on 31/08/16 via Data Protectors Forum and directly to Managers in key areas to provide to relevant staff.	Continues to be implemented	Continues to be implemented	Continues to be implemented			Ongoing/Adhoc	Jul-18	Checklist includes this	Complete-ongoing with monitoring	IAO's
11	**11. Data protection officer's (DPO's)**												
11.1	**Data Protection officer**	Designating a data protection officer- Article 37-39 and assess where this role will sit within our organisation's structure and governance arrangements. Prepare report for CMT approval and appoint to role before May 18. Determine position in governance structure and ensure DPO has appropriate expertise.	Appointment of role considered at CMT on 17/10/17 and approved. JD drafted and to go to panel in Dec 17.	Job evaluation panel considering Jan 18.	Job approved, to be recruited March-18	Complete post filled 25 March 18			Completed but ongoing		Recruiting March 18	Complete	LDSM
12	**12. International**												
12.1 G	**International supervisory authority (ICO)**	Determine which data protection supervisory authority the council comes under	The council will be under the UK supervisory body which will be the Information Commissioner's Office (ICO)	Ongoing	Ongoing	Complete			Completed but ongoing		Included in the checklist and privacy statements	Complete and monitoring	IGO/LDSM
12.2	**International transfers**	Identify any areas where personal data is being transferred to a third country (outside EU and EEA) and if taking place ensure necessary safeguards are in place.	No areas identified although IT due diligence questions being drafted to include products to hosted in the UK although IT already applying in Polices	No areas identified although IT due diligence questions being drafted to include products to hosted in the UK although IT already applying in IT Policies	No areas identified although IT due diligence questions being drafted to include products to hosted in the UK although IT already applying in IT policies	IT already applying, ensuring any transfers outside EEA are compliant with GDPR through contract variations.			Completed but ongoing			To finalise due diligence IT questions to be raised when procuring products	BDITM

AUDIT COMMITTEE **19 JULY 2018**

SUBJECT:	**AUDIT COMMITTEE AND INTERNAL AUDIT REVIEW OF EFFECTIVENESS**
DIRECTORATE:	**CHIEF EXECUTIVE AND TOWN CLERK**
REPORT AUTHOR:	**JOHN SCOTT, AUDIT MANAGER**

1. Purpose of Report

1.1 To provide information on the review of effectiveness for the Audit Committee and Internal Audit and obtain agreement in terms of the composition of a review group.

2. Executive Summary

CIPFA has recently updated guidance for Audit Committees and a Local Government practice note is also awaited for revised Internal Audit Standards. As a result the Audit Committee terms of reference have been revised which is subject to a separate Committee report in July 2018. Reviews of effectiveness should also be undertaken for both the Audit Committee and Internal Audit against terms of reference, standards and guidance.

3. Background

3.1 CIPFA's 2018 guidance on the function and operation of audit committees in local authorities and police bodies, represents best practice for audit committees in local authorities throughout the UK and for police audit committees in England and Wales. This replaces the previous 2013 Position Statement.

3.2 Internal Audit were subject to a formal external assessment against audit standards in October 2016, however it is still good practice to undertake a periodic internal review of effectiveness.

4. Review

4.1 It is suggested that a review group is formed in September consisting the Chair, Vice Chair and Independent member, plus any other member who may wish to be included. The Chief Financial Officer and Audit Manager will also assist. This review group will report back to the Committee in December 2018.

5. Organisational Impacts

5.1 Finance (including whole life costs where applicable)

There are no direct financial implications

5.2 Legal Implications including Procurement Rules

The review of effectiveness aids compliance with the Accounts and Audit Regulations

6 Recommendation

6.1 Members agree on the composition of the review group.

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	None
List of Background Papers:	None
Lead Officer:	John Scott , Audit Manager Telephone (01522) 873321

AUDIT COMMITTEE **19 JULY 2018**

SUBJECT:	**AUDIT COMMITTEE TERMS OF REFERENCE**
DIRECTORATE:	**CHIEF EXECUTIVE AND TOWN CLERK**
REPORT AUTHOR:	**JOHN SCOTT, AUDIT MANAGER**

1. Purpose of Report

1.1 To obtain comments on an update to the Audit Committee Terms of Reference, following which the updated terms of reference will be presented to Executive and Full Council for approval.

2. Executive Summary

2.1 The Audit Committee terms of reference are based on best practice issued by CIPFA, (Chartered Institute of Public Finance and Accountancy) and the Audit Committee is also referenced within the Public Sector Internal Audit standards.

2.2 CIPFA have recently updated their guidance on Audit Committees including standard terms of reference.

2.3 In order to ensure compliance with agreed standards, this Committee's terms of reference should be amended to reflect this guidance.

3. Background

3.1 CIPFA's guidance on the function and operation of audit committees in local authorities and police bodies, represents best practice for audit committees in local authorities throughout the UK and for police audit committees in England and Wales. This replaces the previous 2013 Position Statement.

3.2 Guidance recognises that audit committees are a key component of governance. The purpose of an audit committee is to provide to those charged with governance independent assurance on the adequacy of the risk management framework, the internal control environment and the integrity of the financial reporting and annual governance processes. Audit committees are an important source of assurance about an organisation's arrangements for managing risk, maintaining an effective control environment and reporting on financial and other performance. The way in which an audit committee is organised will vary depending on the specific political and management arrangements in place in any organisation.

3.3 Audit committees in local authorities and police bodies are necessary to satisfy the wider requirements for sound financial management and internal control. For example in England, the Accounts and Audit (England) Regulations 2015 state that a local authority is responsible "for a sound system of internal control which facilitates the effective exercise of its functions and the achievement of its aims

and objectives; ensures that the financial and operational management of the authority is effective and includes effective arrangements for the management of risk". In addition, in England, Section 151 of the Local Government Act 1972 requires every local authority to "make arrangements for the proper administration of its financial affairs"

4. Changes to Terms of Reference

4.1 The suggested revised terms of reference are attached at Appendix A

4.2 Appendix B, lists all the changes that have been made. This could be a new function, change to an existing function, or maintenance of existing functions where there is no equivalent in the new guidance.

4.3 The key new responsibilities are as follows:

a) Audit Committee Chair to approve significant interim changes to the risk-based internal audit plan and resource requirements followed by report to Audit Committee.

b) To make appropriate enquiries of both management and the Head of Internal Audit to determine if there are any inappropriate scope or resource limitations.

c) To consider any impairments to independence or objectivity arising from additional roles or responsibilities outside of internal auditing of the Head of Internal Audit. To approve and periodically review safeguards to limit such impairments

d) To consider specific reports as agreed with the External Auditor.

e) To support the independence of External Audit through consideration of the External Auditor's annual assessment of its independence and review of any issues raised by PSAA or the authority's auditor panel as appropriate.

f) To monitor progress in addressing risk-related issues reported to the committee.

g) To review the governance and assurance arrangements for significant partnerships or collaborations

4.4 It is not anticipated that these changes will significantly add to the work programme of responsibilities of the Committee. Suggestions as to how these can operate in practice are as follows:

a) Where there is an urgent need to make significant changes, the Chair will be consulted. In other cases a report to Committee will be presented.

b) This can be covered in a statement within each internal audit progress report.

c) This can be considered as part of planning; currently there are no responsibilities outside of internal audit and counter fraud.

d) Where there needs to be a report which sits outside the agreed planned reports.

e) To receive a report on such matters.

f) To consider reports covering any specific risk-related issues outside the standard reporting arrangements.

g) Audit Committee members to consider a separate (future) report on partnership and collaboration assurance.

5. Organisational Impacts

5.1 Finance (including whole life costs where applicable)

There are no direct financial implications.

5.2 Legal Implications including Procurement Rules

These changes in Terms of Reference are in a change in the Council's constitution.

6 Recommendation

6.1 That the Audit Committee comment on the suggested changes and recommend to Executive and Full Council for approval

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	Two
List of Background Papers:	None

Lead Officer: John Scott, Audit Manager
Telephone (01522) 873321

This page is intentionally blank.

9.1 Audit Committee
The Council will appoint an Audit Committee.

9.2 Composition
Audit Committee

(a) The Audit Committee will comprise • seven Councillors • one independent member
(b) The seven councillors of the Audit Committee should include the Chair of Performance Scrutiny Committee.
(c) A member of the Executive may not be a member of this Committee

9.3 Statement of purpose

(a)The Audit Committee will have the following roles and functions:
(b)The audit committee is a key component of the City of Lincoln's corporate governance. It provides an independent and high-level focus on the audit, assurance and reporting arrangements that underpin good governance and financial standards.
(c) The purpose of the Audit Committee is to provide independent assurance to the Council members of the adequacy of the risk management framework and the internal control environment. It provides independent review of the City of Lincoln's governance, risk management and control frameworks and oversees the financial reporting and annual governance processes. It oversees internal audit and external audit, helping to ensure efficient and effective assurance arrangements are in place.
(d) To decide upon and authorise allowances to the Committee's Independent Member.

Governance, risk and control
(a) To consider the council's arrangements to secure value for money and review assurances and assessments on the effectiveness of these arrangements.
(b) To engage with relevant committees to help support ethical values and reviewing arrangements to achieve those values as appropriate
(c) To appoint a Lead Officer to sit on the Information Governance Board responsible for monitoring the Information Governance Strategy and Action Plan.
(d) To monitor the effectiveness of the Authority's risk management Arrangements (development and operation),
(e) To monitor the Council's anti-fraud and anti-corruption arrangements (including an assessment of fraud risks);
(f) To monitor the counter-fraud strategy, actions and resources.
(g) To monitor progress in addressing risk-related issues reported to the committee.
(h) To maintain an overview of the Council's constitution in respect of contract procedure rules and financial procedure rules;

(i) To review any issue referred to it by the Chief Executive, a Strategic Director, Monitoring Officer, Chief Financial Officer or any Council body as the Chair considers appropriate within the general Terms of Reference of the Committee
(j) To review the Authority's assurance statements, including the Annual Governance Statement prior to approval, ensuring it properly reflects the risk environment and supporting assurances (including internal audit's annual opinion on governance, risk and control)
(k) To consider the council's framework of assurance and ensure that it adequately addresses the risks and priorities of the council.
(l) To review the Council's arrangements for corporate governance, including the local Code of Corporate Governance and agreeing necessary actions to ensure compliance with best practice (the good governance framework, including the ethical framework)
(m) To review the governance and assurance arrangements for significant partnerships or collaborations.
(n) To consider the Council's compliance with its own and other published standards and controls;
(o) To report and make recommendations to Executive or Council on major issues and contraventions;
(p) To have rights of access to other Committees of the Council and to strategic functions as it deems necessary.
(q) To receive on an annual basis a report on the Treasury Management Strategy before approval by the Executive and Full Council.
(r) To be responsible for ensuring effective scrutiny of the treasury management strategy and policies.

Internal audit
(a) Receive and consider the annual report and opinion of the Internal Audit Manager including conformance with Internal Audit Standards
(b) Review a summary of internal audit activity including internal audit reports on the effectiveness of internal controls, seeking assurance that action has been taken where necessary on the implementation of agreed actions;
(c) To consider summaries of specific internal audit reports as requested by the Audit committee.
(d) To Approve (but not direct) internal audit's risk-based annual audit plan including resource requirements, the approach to using other sources of assurance and any work required to place reliance upon those sources.
(e) Audit Committee Chair to approve significant interim changes to the risk-based internal audit plan and resource requirements followed by report to Audit Committee.
(f) To make appropriate enquiries of both management and the head of internal audit to determine if there are any inappropriate scope or resource limitations.
(g) To consider any impairments to independence or objectivity arising from additional roles or responsibilities outside of internal auditing of the head of internal audit. To approve and periodically review safeguards to limit such impairments
(h) To monitor audit performance, including QAIP results and any non-conformance with PSIAS and LGAN.

(i) To consider whether the non-conformance is significant enough that it must be included in the AGS
(j) Consider the annual review of effectiveness of internal audit to support the AGS, where required to do so by the Accounts and Audit Regulations
(k) To contribute to the Quality Assurance and Improvement Programme and in particular, to the external quality assessment of internal audit that takes place at least once every five years
(l) To receive reports outlining the action taken where the Audit manager has concluded that management has accepted a level of risk that may be unacceptable to the authority or there are concerns about progress with the implementation of agreed actions
(m) To provide free and unfettered access to the audit committee chair for the head of internal audit, including the opportunity for a private meeting with the committee.
(n) To have the right to call any officers or Members of the Council as required to offer explanation in the management of internal controls and risks.
(o) To approve the internal audit charter.

External audit
(a) To consider the reports of external audit and inspection agencies, including the external auditor's annual letter, relevant reports, and the report to those charged with governance
(b) To consider specific reports as agreed with the external auditor.
(c) To advise and recommend on the effectiveness of relationships between external and internal audit, inspection agencies and other relevant bodies, and that the value of the audit process is actively promoted;
(d) To comment on the scope and depth of external audit work and to ensure it gives value for money.
(e) To support the independence of external audit through consideration of the external auditor's annual assessment of its independence and review of any issues raised by PSAA or the authority's auditor panel as appropriate.
(f) To review proposals made in relation to the appointment of external providers of internal audit services and to make recommendations.
(l) To commission work from internal and external audit, as required, and as resources allow;

Financial reporting

(a) The Audit Committee, as the Committee "Charged with Governance" should consider the external auditor's report to those charged with governance on issues arising from the audit of the accounts
(b) To review the annual statement of accounts. The Committee should consider whether appropriate accounting policies have been followed and whether there are any concerns arising from the financial statements or from the audit that need to be brought to the attention of the Council.
c) The Committee will monitor management action in response to any issues raised by external audit

Accountability arrangements

(a) To report to full council on an annual basis on the committee's performance in relation to the terms of reference and the effectiveness of the committee in meeting its purpose.

9.4 Proceedings of the Audit Committee
(1) The Audit Committee must conduct its proceedings in accordance with Rules 6-8, 12.3 to 12.7, 14 -17 and 18-28 (but not Rule 23.1 or 26 of the Council Procedure Rules set out in Part 4 of this Constitution.

9.5 Quorum
Audit Committee
The quorum for any meeting of the Audit Committee shall be three Councillors.

Appendix B – Changes to the Audit Committee terms of reference

	Existing TOR	Suggested Revised TOR	New Guidance Text
1	Receive and consider the annual report and opinion of the Internal Audit Manager including conformance with Internal Audit Standards	No change suggested *PSIAS and Opinion covered in a separate section* See 8 and 9 below	20 To consider the head of internal audit's annual report: a) The statement of the level of conformance with the PSIAS and LGAN and the results of the QAIP that support the statement – these will indicate the reliability of the conclusions of internal audit. b) The opinion on the overall adequacy and effectiveness of the council's framework of governance, risk management and control together with the summary of the work supporting the opinion – these will assist the committee in reviewing the AGS.
2	Review a summary of internal audit activity including internal audit reports and main issues arising, seeking assurance that action has been taken where necessary;	Change suggested Review a summary of internal audit activity including internal audit reports on the effectiveness of internal controls, seeking assurance that action has been taken where necessary on the implementation of agreed actions;	To consider reports on the effectiveness of internal controls and monitor the implementation of agreed actions. To consider reports from the head of internal audit on internal audit's performance during the year, including the performance of external providers of internal audit services. These will include: a) updates on the work of internal audit including key findings, issues of concern and action in hand as a result of internal audit work (see 8 below)

			b) regular reports on the results of the QAIP (see 8 below) reports on instances where the internal audit function does not conform to the PSIAS and LGAN, considering whether the non-conformance is significant enough that it must be included in the AGS.(see 8 below)
3	To consider summaries of specific internal audit reports as requested by the Audit committee, including the effectiveness of internal control	Change suggested To consider summaries of specific internal audit reports as requested by the Audit committee.	To consider summaries of specific internal audit reports as requested
4	Approve (but not direct) internal audit's annual plan and resource requirements, the approach to using other sources of assurance and any work required to place reliance upon those.	Change suggested To Approve (but not direct) internal audit's risk-based annual audit plan including resource requirements, the approach to using other sources of assurance and any work required to place reliance upon those sources.	To approve the risk-based internal audit plan, including internal audit's resource requirements, the approach to using other sources of assurance and any work required to place reliance upon those other sources.
5		NEW Audit Committee Chair to approve significant interim changes to the risk-based internal audit plan and resource requirements followed by report to Audit Committee.	To approve significant interim changes to the risk-based internal audit plan and resource requirements.
6		NEW To make appropriate enquiries of both management and the head of internal audit to determine if there are any inappropriate scope or resource limitations.	To make appropriate enquiries of both management and the head of internal audit to determine if there are any inappropriate scope or resource limitations.

7		NEW To consider any impairments to independence or objectivity arising from additional roles or responsibilities outside of internal auditing of the head of internal audit. To approve and periodically review safeguards to limit such impairments	To consider any impairments to independence or objectivity arising from additional roles or responsibilities outside of internal auditing of the head of internal audit. To approve and periodically review safeguards to limit such impairments
8	To monitor audit performance and consider the annual review of effectiveness of internal audit.	Change suggested To monitor audit performance, including QAIP results and any non-conformance with PSIAS and LGAN. To Consider whether the non-conformance is significant enough that it must be included in the AGS See also 1 above	To consider reports from the head of internal audit on internal audit's performance during the year, including the performance of external providers of internal audit services. These will include: a) updates on the work of internal audit including key findings, issues of concern and action in hand as a result of internal audit work b) regular reports on the results of the QAIP c) reports on instances where the internal audit function does not conform to the PSIAS and LGAN, considering whether the non-conformance is significant enough that it must be included in the AGS.
9	To monitor audit performance and consider the annual review of effectiveness of internal audit.	Change suggested Consider the annual review of effectiveness of internal audit to support the AGS, where required to do so by the Accounts and Audit Regulations	To consider a report on the effectiveness of internal audit to support the AGS, where required to do so by the Accounts and Audit Regulations
10	To receive reports which provide assurance that action is being taken on risk-related issues and recommendations identified by auditors and inspectors;	Suggested change To monitor progress in addressing risk-related issues reported to the committee.	To monitor progress in addressing risk-related issues reported to the committee.

12	To consider the reports of external audit and inspection agencies, including the external auditor's annual letter, relevant reports, and the report to those charged with governance;	No change	To consider the external auditor's annual letter, relevant reports and the report to those charged with governance.
13		NEW To consider specific reports as agreed with the external auditor.	To consider specific reports as agreed with the external auditor.
14	To advise and recommend on the effectiveness of relationships between external and internal audit, inspection agencies and other relevant bodies, and that the value of the audit process is actively promoted;	No change	To advise and recommend on the effectiveness of relationships between external and internal audit and other inspection agencies or relevant bodies
15	To comment on the scope and depth of external audit work, through plans and reports to ensure it gives value for money;	Change suggested To comment on the scope and depth of external audit work and to ensure it gives value for money.	To comment on the scope and depth of external audit work and to ensure it gives value for money.
16		NEW To support the independence of external audit through consideration of the external auditor's annual assessment of its independence and review of any issues raised by PSAA or the authority's auditor panel as appropriate.	To support the independence of external audit through consideration of the external auditor's annual assessment of its independence and review of any issues raised by PSAA or the authority's auditor panel as appropriate.
17	To liaise with the Audit Commission (or its successor) over the appointment of the Council's external auditor;	Change suggested To review proposals made in relation to the appointment of external providers of internal audit services and to make recommendations.	To review proposals made in relation to the appointment of external providers of internal audit services and to make recommendations.

18	To commission work from internal and external audit, as required, and as resources allow;	No change	To commission work from internal and external audit.
19	To support the development of effective communication with the Assistant Director responsible for Internal Audit and also the Audit Manager and to meet privately with the Audit Manager and / or the External Auditor where required;	Change suggested To provide free and unfettered access to the audit committee chair for the head of internal audit, including the opportunity for a private meeting with the committee.	To provide free and unfettered access to the audit committee chair for the head of internal audit, including the opportunity for a private meeting with the committee.
20	To have the right to call any officers or Members of the Council as required to offer explanation in the management of internal controls and risks.	No change	No equivalent
21	To engage with relevant committees to help support ethical values and reviewing arrangements to achieve those values as appropriate.	No change	No equivalent
22	To decide upon and authorise allowances to the Committee's Independent Member.	No change	No equivalent
23	(s) To appoint a Lead Officer to sit on the Information Governance Board responsible for monitoring the Information Governance Strategy and Action Plan.	Change Officer to Member	No equivalent
24	To monitor the effectiveness of the Authority's risk management arrangements, the control environment and associated anti-fraud and anticorruption arrangements (including an assessment of fraud risks);	Change suggested To monitor the effectiveness of the Authority's risk management Arrangements (development and operation), To monitor the Council's and associated anti-fraud and anti-corruption arrangements	To monitor the effective development and operation of risk management in the council. To review the assessment of fraud risks and potential harm to the council from fraud and corruption.

		(including an assessment of fraud risks); To monitor the counter-fraud strategy, actions and resources.	To monitor the counter-fraud strategy, actions and resources.
25		NEW To monitor progress in addressing risk-related issues reported to the committee.	To monitor progress in addressing risk-related issues reported to the committee.
26	To maintain an overview of the Council's constitution in respect of contract procedure rules and financial procedure rules;	No change	No equivalent
27	To review any issue referred to it by the Chief Executive, a Strategic Director, Monitoring Officer or any Council body as the Chair considers appropriate within the general Terms of Reference of the Committee;	Change suggested To review any issue referred to it by the Chief Executive, a Strategic Director, Monitoring Officer, **Chief Financial Officer** or any Council body as the Chair considers appropriate within the general Terms of Reference of the Committee	No equivalent
28	To review the Authority's assurance statements, including the Annual Governance Statement prior to approval, ensuring it properly reflects the risk environment and supporting assurances (including internal audit's annual opinion	Change suggested To review the Authority's assurance statements, including the Annual Governance Statement prior to approval, ensuring it properly reflects the risk environment and supporting assurances (including internal audit's annual opinion on governance, risk and control)	To review the AGS prior to approval and consider whether it properly reflects the risk environment and supporting assurances, taking into account internal audit's opinion on the overall adequacy and effectiveness of the council's framework of governance, risk management and control.
29	To review the Council's arrangements for corporate governance,	Change suggested	To review the council's corporate governance arrangements against the

	including the Code of Corporate Governance and agreeing necessary actions to ensure compliance with best practice;	To review the Council's arrangements for corporate governance, including the local Code of Corporate Governance and agreeing necessary actions to ensure compliance with best practice (the good governance framework, including the ethical framework)	good governance framework, including the ethical framework and consider the local code of governance.
30		NEW To review the governance and assurance arrangements for significant partnerships or collaborations.	To review the governance and assurance arrangements for significant partnerships or collaborations.
31	To consider the Council's compliance with its own and other published standards and controls;	No change	No equivalent
32	To report and make recommendations to Executive or Council on major issues and contraventions;	No change	No equivalent
33	To have rights of access to other Committees of the Council and to strategic functions as it deems necessary.	No change	No equivalent
34	To receive on an annual basis a report on the Treasury Management Strategy before approval by the Executive and Full Council.	No change	No equivalent (although optional - part of wider remit)
35	To be responsible for ensuring effective scrutiny of the treasury management strategy and policies.	No change	No equivalent (although optional – part of wider remit)
36	To report to full council on an annual basis on the committee's performance in relation to the terms of reference and the effectiveness of the	No change	To report to those charged with governance on the committee's findings, conclusions and recommendations concerning the adequacy

	committee in meeting its purpose. *(NB the audit committee is the committee charged with governance)*		and effectiveness of their governance, risk management and internal control frameworks, financial reporting arrangements, and internal and external audit functions. To report to full council on a regular basis on the committee's performance in relation to the terms of reference and the effectiveness of the committee in meeting its purpose. To publish an annual report on the work of the committee.
37	The Audit Committee, as the Committee "Charged with Governance" should consider the external auditor's report to those charged with governance on issues arising from the audit of the accounts. (There are specific requirements linked to International Auditing Standards and those charged with governance).	Change suggested The Audit Committee, as the Committee "Charged with Governance" should consider the external auditor's report to those charged with governance on issues arising from the audit of the accounts	To consider the external auditor's report to those charged with governance on issues arising from the audit of the accounts.
38	The Committee will monitor management action in response to any issues raised by external audit.	No change	No equivalent

AUDIT COMMITTEE **19 JULY 2018**

SUBJECT:	**APPOINTMENT OF EXTERNAL AUDITOR**
DIRECTORATE:	**CHIEF EXECUTIVE AND TOWN CLERK**
REPORT AUTHOR:	**JACLYN GIBSON, CHIEF FINANCE OFFICER**

1. Purpose of Report

1.1 To present to the Audit Committee the outcome of the process to appoint an external auditor for the Council with effect from 1 April 2018.

2. Executive Summary

2.1 The transitional arrangements in respect of the appointment of the Council's external auditors, currently KMPG LLP, are due to come to an end following the audit of the 2017/18 accounts.

2.2 The Council, in 2017 agreed to opt into the appointing persons arrangements made by the Public Sector Audit Appointments (PSAA) for the appointment of its external auditors.

2.3 Following a tender process to procure the audit services the PSAA have appointed Mazars LLP as the Council's external auditor for five years from 2018/19, with the appointment commencing on 1 April 2018. This represents a change from the existing appointed auditor; KPMG LLP.

3. Background

3.1 The Local Audit and Accountability Act 2014 brought to a close the Audit Commission and established transitional arrangements for the appointment of external auditors and the setting of audit fees for principal local government bodies. These transitional arrangements were set for the period to include the audit of the 2017/18 accounts.

3.2 The Council's current external auditor is KPMG LLP, this appointment having been made under the transitional arrangements.

3.2 In July 2016 the PSAA was selected by the Secretary of State for Communities and Local Government to take on the role of Appointing Person for principal local government bodies for the audit of accounts from 2018/19 onwards. After consideration by the Audit Committee, on 28 February 2017 Council resolved to accept the invitation to opt into the appointing persons arrangements made by PSAA for the appointment of external auditors.

4. Local auditor appointment process

4.1 A total of 483 bodies (98%) of eligible bodies (including police bodies) opted into the sector-led approach offered by PSAA.

4.2 During the period February to June 2017 the PSAA managed a tender process to procure audit services, the total volume of audit work was divided into six contract lots, with the size of the lots graduated to incentivise competing bids. The procurement process has been hailed as highly successful, delivering a reduction in the scale fees payable by local bodies.

4.3 The successful contractors, together with their estimated lot values, are listed below:

- Lot 1 of approx. £14.6 million per audit year was awarded to Grant Thornton LLP;
- Lot 2 of approx. £10.9 million per audit year was awarded to EY LLP;
- Lot 3 of approx. £6.6 million per audit year to awarded to Mazars LLP;
- Lot 4 of approx. £2.2 million per audit year to awarded to BDO LLP;
- Lot 5 of approx. £2.2 million per audit year to awarded to Deloitte LLP; and,
- Lot 6 with no guaranteed value of work to awarded to a consortium of Moore Stephens LLP and Scott-Moncrieff LLP.

4.4 On 14 August 2017, the Council received communication from PSAA of the intention to appoint Mazars LLP as its auditor for five years from 2018/19, with the appointment commencing on 1 April 2018. This represents a change from the existing appointed auditor; KPMG LLP. The communication is attached at Appendix A for information.

4.5 The Council had the opportunity to make representations to PSAA on the proposed appointment, with the following provided as acceptable reasons:

- There is an independence issue in relation to the firm proposed as the auditor, which had not been previously notified to PSAA;
- There are formal and joint working arrangements relevant to the auditor's responsibilities, which had not been previously notified to PSAA; or
- There is another valid reason, for example you can demonstrate a history of inadequate service from the proposed firm.

4.6 There were considered to be no reasons for the Council to make such representations on the appointment and as such the Chief Executive wrote to PSAA on behalf of the Council to accept the appointment of Mazars LLP in September 2017.

4.7 PSAA have subsequently confirmed the appointment of Mazars LLP as the Council's external auditor to audit its accounts for five years, from 2018/19 to 2022/23.

4.8 The appointment of Mazars LLP as the Council's external auditor excludes the Housing Benefits Certification work, this was not included in the scope of works for the PSAA and must be procured separately. The Department for Work and

Pensions (DWP) has now assumed responsibility for issuing guidance and providing support for this assurance process. The Council is currently undertaken a separate procurement process for this element of assurance work.

5. Strategic Priorities

5.1 There are no direct implications for the Council's strategic priorities. The appointment of an external auditor is a statutory requirement of the Council and as such contributes towards the fitness for purpose of the Council's governance arrangements.

6. Organisational Impacts

6.1 Finance

As a result of the bulk procurement for opted in bodies a reduction in audit fees from 2017/18 of 23% has been achieved. The proposed scale fee for the audit of the accounts and VFM conclusion for 2018/19 is £36,332 in comparison to £47,185 for 2017/18.

Once the procurement for the Housing Benefits Certification work is complete and the contract value is known the overall budget saving will be clear.

6.2 Legal Implications including Procurement Rules

Section 7 of the Local Audit and Accountability Act 2014 requires a relevant authority to appoint a local auditor to audit its accounts for a financial year not later than 31 December in the preceding year.

Section 17 gives the Secretary of State the power to make regulations in relation to an 'appointing person' specified by the Secretary of State. This power has been exercised in the Local Audit (Appointing Person) Regulations 2015 and this gives the Secretary of State the ability to enable a sector led body to become the appointing person.

The appointment of Mazars LLP has been made under regulation 13 of the Local Audit (Appointing Person) Regulations 2015, and was approved by the PSAA Board at its meeting on 14 December 2017.

7. Risk Implications

7.1 The Council has adopted a sector led approach, through PSAA, to the appointment of the new external auditor to ensure a successful transition to the new arrangements in a timely and efficient manner.

8. Recommendation

8.1 The Audit Committee is asked note the appointment by PSAA of Mazars LLP as the external auditor for the Council for a five year period from 1 April 2018.

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	None
List of Background Papers:	Appointment of external auditors, Audit Committee 13 December 2016 and Council 28 February 2017
Lead Officer:	Jaclyn Gibson, Chief Finance Officer Telephone (01522) 873258

This is a formal communication to the chief executive and chief finance officer of City of Lincoln Council to consult on the auditor appointment from 2018/19

I am writing to consult you on the appointment of Mazars LLP to audit the accounts of City of Lincoln Council for five years from 2018/19. The appointment will start on 1 April 2018.

Background
For audits of the accounts from 2018/19, PSAA is responsible for appointing an auditor to principal local government and police bodies that have chosen to opt into its national auditor appointment arrangements. More information on the appointing person scheme is available on our website.

About the proposed appointment
PSAA must, under regulation 13 of the Regulations, appoint an external auditor to each opted-in authority and consult the authority about the proposed appointment.

City of Lincoln Council has opted into PSAA's auditor appointment arrangements. We have sent regular email communications to audited bodies about this process, and wrote to you on 19 June 2017 to advise you that we had completed a procurement to let audit contracts from 2018/19. Mazars LLP was successful in winning a contract in the procurement, and we propose appointing this firm as the auditor of City of Lincoln Council.

Mazars is a large global audit and accounting firm with over 18,000 professionals in 79 countries worldwide. In the UK the firm ranks in the top ten with 1,700 employees and 140 partners working out of 19 offices, and UK fee income in 2016 of £160m.The firm's dedicated public audit team has significant experience in providing external audit to public sector bodies. It comprises individuals with experience of auditing councils, combined authorities, police bodies, fire and rescue authorities, local government pension funds and other public bodies. In addition to its audit contract with PSAA, the firm also has a substantial portfolio of NHS audits and is one of the National Audit Office's framework suppliers for central government audit.

In developing this appointment proposal, we have applied the following principles, balancing competing demands as much as we can, based on the information provided to us by audited bodies and audit firms:

- ensuring auditor independence, as we are required to do by the Regulations;
- meeting our commitments to the firms under the audit contracts;
- accommodating joint/shared working arrangements where these are relevant to the auditor's responsibilities;
- ensuring a balanced mix of authority types for each firm;
- taking account of each firm's principal locations; and
- providing continuity of audit firm if possible, but avoiding long appointments.

Further information on the auditor appointment process is available on our website.

Responding to this consultation
We are consulting you on the proposed appointment of Mazars LLP to audit the accounts of

City of Lincoln Council for five years from 2018/19. The consultation will close at **5pm on Friday 22 September 2017**.

If you are satisfied with the proposed appointment, please confirm this by email to auditorappointments@psaa.co.uk. No further action is needed from you.

The PSAA Board will consider all proposed auditor appointments at its meeting scheduled for 14 December 2017. We will write by email to all opted-in bodies after this Board meeting to confirm auditor appointments.

Process for objecting to the proposed auditor appointment

If you wish to make representations to PSAA about the proposed auditor appointment, please send them by email to auditorappointments@psaa.co.uk to arrive by **5pm on Friday 22 September 2017**.

Representations can include matters that you believe might be an impediment to the proposed firm's independence, were it to be your appointed auditor. Your email should set out the reasons why you think the proposed appointment should not be made. The following may represent acceptable reasons:

1. there is an independence issue in relation to the firm proposed as the auditor, which had not previously been notified to PSAA;
2. there are formal and joint working arrangements relevant to the auditor's responsibilities, which had not previously been notified to PSAA; or
3. there is another valid reason, for example you can demonstrate a history of inadequate service from the proposed firm.

We will consider carefully all representations and will respond by Monday 16 October 2017 by email.

If your representations are accepted, we will consult you on an alternative auditor appointment between 16-27 October 2017. If your representations are not accepted, we will confirm this to you. You may choose to make further representations to the PSAA Board, providing any additional information to support your case.

We will write to all bodies to confirm the Board's final decision on the appointment of the auditor before 21 December 2017.

Scale fees for 2018/19

We will consult on scale fees for 2018/19 in due course and will publish confirmed scale fees for 2018/19 for opted-in bodies on our website in March 2018. The results of the audit procurement indicate that a reduction in scale fees in the region of approximately 18 per cent should be possible for 2018/19, based on the individual scale fees applicable for 2016/17. Further information on the audit procurement is available on our website.

Further information

If you have any questions about your proposed auditor appointment or the consultation process, please email us at auditorappointments@psaa.co.uk.

Yours sincerely
Jon Hayes
Chief Officer

Item No. 10

AUDIT COMMITTEE **19 JULY 2018**

SUBJECT:	**REVIEW OF FRAUD SANCTION POLICY**
DIRECTORATE:	**CHIEF EXECUTIVE AND TOWN CLERK**
REPORT AUTHOR:	**MARTIN WALMSLEY, HEAD OF SHARED REVENUES AND BENEFITS**

1. Purpose of Report

1.1 To update the Audit Committee on a small number of amendments to the already adopted Fraud Sanction Policy, in respect of the shared Revenues and Benefits service between City of Lincoln Council and North Kesteven District Council.

2. Executive Summary

2.1 On 12th September 2013, Revenues and Benefits Joint Committee approved an updated version of the shared Benefit Fraud – Sanctions and Prosecutions Policy, making references to the Council Tax Support schemes (which replaced the national Council Tax Benefit scheme from 1st April 2013). The purpose of the policy is to assist the Councils in the shared service in preventing and detecting fraud in a consistent, effective, efficient and equitable manner.

2.2 On 1st October 2014, responsibility for investigation of Housing Benefit fraud in respect of City of Lincoln and North Kesteven transferred to the Single Fraud Investigation Service (SFIS) under Department for Work and Pensions (DWP). However, numerous functions still remain with the local authorities – including;

- Provision of data to SFIS;
- Consideration of Administrative Penalties;
- Investigation of Council Tax Support fraud.

2.3 On 11th February 2016, Executive Board approved an updated Fraud Sanction Policy, to reflect work being undertaken by SFIS and different levels of overpayment value being considered for prosecution.

2.4 The proposed amended policy at Appendix 1, highlights further changes required to the existing policy.

3. Proposed amendments to Fraud Sanction Policy (see Appendix 1)

3.1

- Paragraph 5.1.1: 'Panel' amended to 'Benefits Team Leader' (x4);
- Paragraph 5.1.1: Existing policy states '…will consider cases for sanction…', amended to '…will consider cases for either a warning or penalty…';
- Paragraph 5.1.2: 'Panel' amended to 'Benefits Team Leader';

Paragraph 5.1.2: 'For offences committed against the council tax support scheme, the penalty is 50% of the amount overpaid with a minimum penalty of £100 and maximum penalty of £1000' amended to '…, 'the penalty is £70.00';

- Paragraph 5.1.3: 'Panel' amended to 'Benefits Team Leader' (x2);
- Paragraph 5.2.1: 'Panel' amended to 'Benefits Team Leader';
- Paragraph 5.2.2: 'Panel' amended to 'Benefits Team Leader';
- Paragraph 5.3.3: Inserted new paragraph; The Crown Prosecution Service will require a Witness Statement in each case that is taken forward for a prosecution at court. This will be provided by a Benefits Team Leader.
- The Executive will also be asked to determine the level of delegation for potential future 'minor amendments', to the Fraud Sanction Policy, which may be delegated to officers – for example, a change in job title/role making decisions on sanction, or a legislative change in a £ cost which may be applied

3.2 The revised policy is to go through the consideration/approval process, as follows:

City of Lincoln Council	North Kesteven District Council
Policy Scrutiny Committee: - 19th June 2018	Performance and Resources Overview and Scrutiny Panel: - 18th June 2018
Audit Committee - 19th July 2018	
Executive: - 23rd July 2018	Executive Board: - 26th July 2018

3.3 Policy Scrutiny Committee resolved that the amendments to the Fraud Sanctions Policy be supported

4. Strategic Priorities

4.1 Both City of Lincoln and North Kesteven have a number of strategic priorities. Two that have an impact on the Revenues and Benefits Service are:-

- Lincoln: "Let's Reduce Inequality".
- North Kesteven: "Our Community Our Economy".

4.2 The Benefits Service plays a key role in reducing inequality by ensuring residents receive the benefits they are entitled to and providing money / debt advice. The Revenues Section is also mindful of the strategic priorities when engaging with business ratepayers as they recover business rates – and also promoting and encouraging growth in the districts. Digital Inclusion, Channel Shift / Customer Experience, Financial Inclusion and Partnership Working are all key priorities for the shared service.

5. Organisational Impacts

5.1 Finance: There are no significant financial costs involved in the amendments proposed to this policy, although they will help to allow more effective and efficient use of officer time.

5.2 Legal Implications including Procurement Rules: There are no direct Legal or Procurement implications arising from this report.

5.3 Equality, Diversity & Human Rights: There are no direct implications arising from this report.

6. Risk Implications

6.1 A Risk Register is in place for the Revenues and Benefits shared service.

7. Recommendations

7.1 Audit Committee note the proposed amendments to the Fraud Sanction Policy.

Is this a key decision?	Yes/~~No~~
Do the exempt information categories apply?	~~Yes~~/No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	~~Yes~~/No
How many appendices does the report contain?	One
List of Background Papers:	None

Lead Officer: Martin Walmsley, Head of Shared Revenues and Benefits
Telephone (01522) 873597

This page is intentionally blank.

City of Lincoln Council

&

North Kesteven District Council

Benefit fraud, sanctions and prosecutions policy

CONTENTS

1. Background

1.1 On 1st June 2011 the City of Lincoln and North Kesteven District Councils entered into an arrangement to share the provision of revenues and benefits services between them. By sharing their services the Councils are seeking to achieve savings and efficiencies.

1.2 From 1st October 2014, transfer of Housing Benefit Fraud investigation transferred from City of Lincoln Council and North Kesteven Council to the Department for Work and Pensions (DWP) under the Single Fraud Investigations Service. City of Lincoln Council and North Kesteven District Council retain responsibility for investigating potentially incorrectly-claimed Council Tax Support.

1.3 For the purposes of this policy, a person is considered to commit benefit fraud if they commit or attempt to commit a statutory offence against any of the following schemes operated by the Councils:

- Housing Benefit;
- Council Tax Benefit;
- Council Tax Support;
- any successor benefit to these schemes.

2. Statement of Intent

2.1 The City of Lincoln and North Kesteven District Councils are committed to protecting public funds by taking action to combat benefit fraud. The Councils will not tolerate any form of benefit fraud, whether it is attempted from within or outside of the Councils. If there is sufficient evidence to show that a claimant or some other third party has committed benefit fraud, the Councils will consider taking action against that person under the appropriate legislation.

2.2 The Councils will seek to recover any benefit overpaid as a result of fraudulent activity and will use every power available to them to minimise the loss to the public purse through fraud.

3. Action to counter fraud

3.1 The Councils are committed to operating in an open and honest way in order to:

- encourage the prevention of fraud;
- promote the detection of fraud;

- deter people from committing fraud by prosecuting or issuing sanctions against people caught committing benefit fraud.

4. The prevention and detection of fraud

4.1 The prevention of fraud

4.1.1 The Councils will seek to prevent fraud from entering the benefits system by:

- requiring appropriate verification of evidence and details provided by claimants to obtain benefit;
- carrying out risk based reviews of claims, as required;
- publicising the Councils' involvement in data matching and other counter fraud activities;
- participating and contributing to the Regional Boards for fraud;
- working with SFIS to facilitate the effective detection of Benefit Fraud;
- providing reliable and timeous data to the DWP on anti fraud activity and sanction and prosecution outcomes;
- promoting and providing means for members of the public to report cases of suspected fraud to the Councils;
- work with SFIS to facilitate delivery of anti-fraud training to Council staff, as appropriate;
- in partnership with SFIS, publicising successes in detecting fraud and delivering sanctions and prosecutions to deter others from committing similar fraudulent acts.

4.2 The detection of fraud

4.2.1 The Councils will seek to detect fraud by:

- working with partners to facilitate delivery of an effective fraud investigation service to ensure that irregularities and fraudsters are identified and dealt with appropriately;
- providing caseload information to the Secretary of State for Work and Pensions for data matching, risk analysis and identification or irregularities;
- participating in anti fraud activities such as the National Fraud Initiative (NFI);

- participating in the annual Housing Benefit Review conducted by the DWP which involves a statistically valid sample of the caseload being reviewed in depth by Secretary of State appointed inspectors to evaluate the level of fraud and error in the regional and national caseload and helps the Council to plan its risk profile;
- complying with Police and Criminal Evidence Act, Regulation of Investigatory Powers Act, Social Security Acts, Data Protection Act and other relevant legislation in managing anti-fraud activity;
- provide a 'Single Point of Contact' (SPOC) for SFIS for management of fraud matters;
- provide a SPOC for secure transfer of data to/from SFIS;
- monitoring fraud referrals, investigation activity and sanction and prosecution outcomes to develop and identify high risk areas for anti fraud exercises.

4.3 Duties and considerations of employees and elected members

4.3.1 The Councils expect officers to report details of any property that they are renting to tenants and any claims to benefit to which they have some connection. This may be a claim to benefit where an officer or member is the landlord, claimant, partner, dependant or non dependant of the claim. Any interest in a claim to benefit by officers and members must be recorded in the Register of Interests in the usual manner.

4.3.2 Any officer involved in the administration of benefits who has knowledge of a claim where they are a close family member of the claimant or partner (as defined in regulation 2 of the Housing Benefit General Regulations) must report this connection to the Head of Shared Revenues and Benefits. Officers involved in the administration of revenues and benefits may be required to complete a declaration periodically about these issues.

4.3.3 Any officer found to be involved in an offence under the Social Security Administration Act 1992 (as amended), or any other criminal offence involving claims to benefit at either of the Councils, or any other Council or Government Department, must report this to the Head of Shared Revenues and Benefits. In addition to any prosecution proceedings that result from the benefit fraud, the Councils may take disciplinary action.

4.4 Duties and considerations of investigation officers

4.4.1 Whilst investigating benefit/support fraud, the Councils' investigation officers and authorised officers will work within the guidelines of the Police and Criminal Evidence Act 1984, Criminal Procedures and Investigation Act 1996, the

Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Social Security Acts and subsequent amendments, any new legislation introduced to govern this area of work and the Councils' policies on customer care.

4.4.2 Officers will operate within the confines of the Data Protection Act 1998 and will maintain client confidentiality.

4.4.3 The Councils will investigate any instances where an officer has abused their powers whilst investigating any allegation of benefit/support fraud. If the investigation reveals breaches of the law or Council policy then disciplinary action may take place.

4.5 Resources

4.5.1 If required at any time, The Head of Paid Service will appoint at least one "Authorised Officer" under Section 110A of the Social Security Administration Act 1992 and Regulation 3 of the Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013.

4.5.2 The Authorised Officer may exercise any of the powers that are conferred by Section 109B and 109C of the Social Security Administration Act 1992 and Regulations 4 and 5 of the Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013. Authorised Officers exercise powers to obtain information to assist in an investigation. Obstruction of such an officer or failure to produce information is an offence and the Council may take action against any person who commits it.

4.5.3 The Head of Paid Service will ensure that the Authorised Officers are fit and proper persons to be authorised and will issue those persons with a certificate of appointment.

5. Sanctions and Prosecutions

5.1 The decision making process

5.1.1 A Benefits Team Leader will consider in each case recommended for further action when the evidence is sufficient to suggest that an alleged offender would be found guilty if the case were placed before the Court. A Benefits Team Leader will consider whether further action should be taken in those cases proven and which sanction, if any, should be applied. A record of the reasons for the decision will be made. As Housing Benefits investigation is now a function under DWP through SFIS, the evidence provided and case summaries will be the responsibility of SFIS. A Benefits Team Leader will provide an audit

trail of decisions made. For Council Tax Support only cases, a Benefits Team Leader will consider cases for either a warning or a penalty to be placed on their Council Tax account and follow the same process (but without SFIS) – which could include other partners, for example other local authorities assisting with this function.

5.1.2 The courses of action available to the Benefits Team Leader are as follows:

- Prosecution through the Courts

  The offender may be prosecuted through either the Crown or Magistrates Court, dependant upon the severity of the case and if found guilty will face a maximum sentence of seven years in prison, or a fine, or both for the most serious offences;

- Administrative penalty

  As an alternative to prosecution, the offender may agree to repay an extra financial penalty instead of facing prosecution. The amount of the penalty is specified by law, but varies dependent upon the period of the offence and the scheme against which the offence has been perpetrated:

  - for offences against the housing and council tax benefit schemes committed in part or in whole prior to 8th May 2012, the penalty is 30% of the amount overpaid;
  - for offences against the housing benefit and council tax benefit schemes committed wholly after 7th May 2012, the penalty is 50% of the amount overpaid, with a minimum penalty of £350 and a maximum penalty of £2000;
  - for offences committed against the council tax support scheme, the penalty is £70.00.

5.1.3 The Benefits Team Leader can decide to take no action in respect of any case. If this occurs a record of the Benefits Team Leader's reasons for reaching this decision will be recorded.

5.1.4 In all cases, the claimant will be expected to repay any amount of benefit overpaid.

5.2 Factors to consider

5.2.1 The Benefits Team Leader will take the following factors into account when deciding whether it is in the public interest to prosecute someone whom it is alleged has committed benefit fraud:

- the amount of any overpayment of Housing Benefit, Council Tax Benefit or Council Tax Support, or any successor benefit made as a consequence of the fraud;

- the amount of any overpayment of any other social security benefit, or loss to public funds, made as a consequence of the fraud;
- the physical and mental condition of the alleged offender;
- the number and type of offences it is alleged to have been committed and the length of time over which the offences have taken place;
- any voluntary disclosure;
- the level of co-operation offered by the alleged suspect during the investigation;
- any relevant social factors such as age, health, employment, family commitments, financial issues, and any other issues that are felt to be relevant;
- the strength of the evidence;
- any failings in the investigation;
- any failings in the administration of the claim that could have contributed to the alleged offence;
- any exceptional or unusual factors specific to the case;
- any mitigating factors brought to the attention of the Council;
- any admission or denial of the offence by the alleged offender;
- any refusal to accept an administrative penalty or caution;
- any previous proven history of committing benefit fraud offences.

5.2.2 In deciding which sanction is appropriate, the Benefits Team Leader will take account of the following guidelines. These guidelines are based upon Department for Work and Pensions research and practice and local experience. Each case will be considered on its own merits and the guidelines are not binding.

5.2.3 If the overpayment of benefit is under £2,000, the Council will generally seek to offer an administrative penalty, unless when considering the other factors, prosecution is more appropriate. The Council will also give consideration to DWP overpayment amounts for prosecution, which SFIS will liaise and update the Councils regarding as and when these guideline-limits change.

5.2.4 If the overpayment of benefit is over £2,000, the Council will generally seek to prosecute the offender, unless when considering the other factors an alternative to prosecution would be more appropriate. The Council will also give consideration to DWP overpayment amounts for prosecution, which SFIS will liaise and update the Councils regarding as and when these guideline-limits change.

5.2.5 The option will remain to take prosecution action in any case if aggravating circumstances exist, including attempted fraud, irrespective of the level of overpayment involved.

5.3 Delivering sanctions and prosecutions

5.3.1 Prosecutions will generally be taken by the Criminal Prosecution Service where the case has been investigated by SFIS

5.3.2 In some cases, it may be appropriate for another local authority to administer the sanction, if for example, the alleged offender has moved away and is resident in another local authority area – or the Councils are working with another local authority on investigative functions delivery.

5.3.3 The Crown Prosecution Service will require a Witness Statement in each case that is taken forward for a prosecution at court. This will be provided by a Benefits Team Leader.

5.4 Publicity

5.4.1 The Councils may seek publicity about successful benefit fraud prosecutions. The aim of such publicity is to deter others from committing similar frauds and to demonstrate to taxpayers that the Councils are protecting public funds.

This page is intentionally blank.

Item No. 12

AUDIT COMMITTEE **19 JULY 2018**

SUBJECT:	**AUDIT COMMITTEE WORK PROGRAMME**
REPORT BY:	**JOHN SCOTT, AUDIT MANAGER**

1. Purpose of Report

1.1 To provide details of the draft Audit Committee work programme for 2018/19

2. Executive Summary.

2.1 The Audit Committee approves a work programme each year and monitors progress.

3. Main report

3.1 The proposed work programme is attached at Appendix A. The frequency of meetings has been reviewed and is considered appropriate for 2018/19.

4. Organisational Impacts

4.1 Finance
There are no direct financial implications arising as a result of this report.

4.2 Legal Implications including Procurement Rules
There are no direct legal implications arising as a result of this report.

4.3 Equality, Diversity & Human Rights
There are no direct E and D implications arising as a result of this report.

5. Recommendation

5.1 The Audit Committee should comment on and agree the work programme for 2018/19.

Key Decision	No
Do the Exempt Information Categories Apply?	No
Call in and Urgency: Is the decision one to which Rule 15 of the Scrutiny Procedure Rules apply?	No

How many appendices does the report contain?	One
List of Background Papers:	None
Lead Officer:	Audit Manager Telephone 873321

AUDIT COMMITTEE
AUDIT WORK PROGRAMME FOR 2018/19

Meeting dates	Audit Items	Training (Suggested)	Comments
14th June 2018	• Internal Audit Progress report • Statement of Accounts (Draft) • Annual Governance Statement (Draft review) • Audit Committee Work Programme • Annual Internal Audit Report • 12 month Fraud and Error report	• Audit Committee effectiveness (new members) • Local Government Financial Statements explained • Annual Governance Statement/Corporate Governance (Part of Meeting)	
19 Jul 2018 6.00 pm	• Statement of Accounts / Annual Governance Statement (Final) • Annual Governance Report / Auditors Report (External Audit) • Terms of Reference review - Audit Committee • Review of the effectiveness of Internal Audit and Audit Committee • Appointment of External Auditor		
27 Sep 2018 6.00 pm	• Internal Audit progress report • Audit Committee Work Programme • Information Governance – update report • Annual Governance Statement monitoring report • Annual Complaints report		

	• **Terms of Reference review – Internal Audit**		
18 Dec 2018 6.00 pm	• **Annual Audit Letter (External Audit)** • **Internal Audit progress report** • **Six Month Fraud and Error report** • **Annual Governance Statement - monitoring** • **Audit Committee Work Programme** • **Counter fraud policies** • **Information Governance Update** • **Review of the effectiveness of Internal Audit and Audit Committee**	• **Counter Fraud**	
12 Feb 2019 6.00 pm	• **Internal Audit Progress report** • **Treasury management policy and strategy (consultation prior to approval by Council)** • **Audit Committee Work Programme** • **External Audit annual report on grants and returns** • **External Audit plan** • **Draft Internal Audit plan 19-20**	• **Treasury Management**	
26 Mar 2019 6.00 pm	• **Internal Audit Progress report** • **Combined Assurance report** • **Annual Governance Statement –update report** • **Final Internal Audit Strategy and Plan 19-20** • **Risk Management Strategy / annual report**		

	• **Statement on Accounting Policies** • **Audit Committee Work Programme** • **External Audit Inquiries – 18/19 Statement of Accounts** • **IAS19 – Assumptions used to calculate pension entries in the Statement of Accounts and Audit Regulations** • **Strategic Fraud risk register** • **Information Governance Update report**		

A private meeting between the Audit Committee and internal and external audit managers can be arranged outside of the meeting agenda times.

This page is intentionally blank.