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 4
1. Purpose 4
2. Scope 4
3. Policy 5
   3.1. The Data Protection Principles 5
   3.2. Responsibilities 6
   3.3. Engaging a data Processor to process personal data on behalf of the council 7
4. Rights of individuals and information access requests 8
   4.1 Right to be informed 8
   4.2 The right to access 8
   4.3 The right to rectification 9
   4.4 The right to erasure 9
   4.5 The right to restrict processing 10
   4.6 The right to data portability 10
   4.7 The right to object 11
   4.8 Rights related to automated decision making and profiling 11
   4.9. Exemptions to individual's information rights 12
5. Disclosure of personal information about third parties 12
6. Consent 12
7. Privacy by design and Data Protection Impact Assessments (DPIA's) 13
8. International transfers 13
9. Further information, enquires and complaints 14
10. Breach of the Policy 14
11. Data breach notification 14
12. Policy Compliance 15
   12.1. Compliance Measurement 15
   12.2. Non-Compliance 15
   12.3 Policy Review 15
13. Related Policies, and Guidance 16
14. Definitions 16
   14.1. Abbreviations 16
   14.2. Definitions 16
GDPR and Data Protection Policy- Appendix 1 19

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

GDPR and Data Protection Policy- Appendix 1

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.