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

1. Purpose of Report

1.1 To update Audit Committee on the progress of Information Management and the continued implementation of the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

2. Background and Progress

2.1 The GDPR Action Plan has been amended to the Information Governance IG/GDPR Ongoing Action Plan attached as Appendix A

2.2 The GDPR Group are prioritising ongoing compliance including building on and improving completed actions however there is a lot of work to be done, particularly in the following areas:-

(a) Training

Action:

Ongoing Data Protection training (Article 5 GDPR- security, Article 32- testing effectiveness of measures for security) and ensure renewed annually or at least every 2 years with non-completion being followed up. Include member training. Implement ongoing training needs plan.

Although progress in this area has been significant (completion at 90.05% for all staff) it is essential that the DP training is renewed as required by all staff/members and automated as far as possible. All new staff receive the training on induction.

Training for new members was delivered May 18 and all Member training October 18. A follow up session for non-attendees is currently being offered to members.

City of Lincoln Council (CLC) have purchased data protection and cyber security videos recommended by Central Government. It has been agreed by Assistant Director (AD) Group that ongoing Data Protection (DP) training will be renewed, updated and delivered to all staff by the videos along with questions to test understanding through policy management software net-consent. The plan is to roll this out in the new year and testing to be carried out on small groups of staff from December 18.

(b) Data Protection Impact Assessments (DPIA)

Action:

DPIA's- 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.

These have been rolled out to various teams to be completed in respect of assessing how we process personal data before a project/piece of work, for example.

Under GDPR these assessments are now mandatory in particular circumstances including retrospectively for core systems processing large amounts of sensitive data. This has also been assisted by an Applications Review of existing systems being undertaken by Audit with relevant actions being followed up by IT and the Data Protection Officer. In relation to new systems we have a DPIA process including, Screening questions, Guidance and Template but take up needs to continue to be promoted and improved. The DPIA process has now been added to the Lincoln Project Management Model. Assessments have also been undertaken as required in relation to new projects involving the sharing between partners of sensitive special category data.

(c) Policies, Guidance and Procedures

Action:

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.

Significant progress has been made in this area. A DPA/GDPR Policy was drafted and approved by Committee then rolled out to all staff to individually acknowledge through netconsent.

All Information Management (IM) Policies have now been updated and approved in light of GDPR and are shortly to be rolled out to all staff through netconsent. It is proposed that Staff simply acknowledge that they are aware the Policies have been updated and where to find them as oppose to individual sign up to each Policy.

(d) 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 include the Crown Commercial Service (CCS) approved GDPR clauses. This project has proven to be resource intensive. This stems from the complexity of the contract variations received from Suppliers which generally do not follow the CCS clauses with Suppliers having instructed legal advisers to draft clauses in their favour in relation to liability, for example and some Suppliers refusing to accept they are processing personal data on our behalf. In relation to CLC contacting Suppliers to vary contracts a project is ongoing where IAO's have declared the contracts and partnerships they have in their areas. These contracts are being prioritised in relation to sensitivity of the data and Suppliers contacted to vary the contracts.

(e) Record of Processing Activities (ROPA)

Action:

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.

CLC has an asset register complied by the DPO after extensive work with Information Asset Owners (IAO's). This needs to be kept up to date by IAO's. The register does include a description of information being shared although this may need to be expanded upon in some areas. There is also software now available from the LGA which could approve these records including the ability for IAO's to access and update these records. More resources are likely to be required from BDIT to develop this.

(f) Individual Rights/Retention

Action:-

Access, rectification, right to be forgotten, data portability- Articles 15-20. 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 Retention and Disposal work.

Guidance and procedures have been successfully implemented to ensure individuals are able to exercise their rights.

The BDIT Manager continues to work on this area in relation to electronic file storage and IT systems however solutions are complex, and options potentially expensive and resource intensive. IAO's are to encourage their teams to review the information they hold in systems, drives and mailboxes and delete any unnecessary information beyond its retention period. IAO's can contact the BDIT Manager for further assistance with this area. BDIT are now piloting a process which aims to help services with this exercise.

Retention and disposals schedules were produced based on the LGA's guidance and rolled out to all staff on the Council's intranet and website.

Implementation is part of IAO's responsibility and compliance by IAO's is self-certified in the annual IAO Checklist.

Systems are complaint with the individual's new rights but in some cases only manually and CLC will need to assess based on the impact on resources of rights requests whether enhanced automation tools need to be purchased going forward.

2.3 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. The GPDR group will consider if any realignment of resources may be necessary and monitor and report progress. However, it may be that additional resources may be required in order expedite some of the more time consuming issues

3. Senior Information Risk Officer (SIRO)

3.1 This role was previously held by the Legal & Democratic Services Manager but given IG sits under the BDIT Manager it makes sense in future for this role to be connected with IG and BDIT. Central Government recommends the SIRO is a board member and the Director of Housing and Investment (previous AD for Strategic Development) has confirmed they would be willing to take on this role for the time being. The SIRO is a champion for good information governance practices, who works closely with the DPO and IT where required in respect of IG/Cyber Security and oversees signing off risk in DPIA's related to this and new technologies where required.

4. AGS

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

5. Vision 2020

5.1 GDPR implementation was one of the Vision 2020 projects to be delivered in year 2018/19. The Working Group was meeting monthly prior to GDPR coming into force in May 2018 to ensure we remained on track with the Action Plan. The Group now meet on a quarterly basis.

6. Strategic Priorities

6.1 <u>High Performing Services</u>

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

7. Organisational Impacts

7.1 Finance (including whole life costs where applicable)

Nothing relevant to this report.

7.2 Legal

As outlined within the report.

7.3 Equality & Diversity and Human Rights

There is no impact arising from this report in this area.

8. Risk Implications

8.1 CLC must comply with the GDPR and DPA data protection legislation. Non-compliance may result in monetary fines, compensation claims and a loss of public and partner trust.

9. Recommendation

9.1 To note the report and attached action plan and to specifically provide comments on the following:-

- The renewal and the follow up of data protection training
- Monitoring and delivery of ongoing actions and resources
- The new appointment of SIRO
- The AGS status of amber

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