GDPR/Data Protection Policy

Report of Monitoring Officer

Date:	14 November 2019
Agenda item:	7
Officer Title:	Christie Tims – Head of Corporate Services and Monitoring Officer
Local Ward Members	N/A

Lichfield district council
www.lichfielddc.gov.uk

Audit and Member Standards Committee

1. Executive Summary

1.1 The General Data Protection Regulation (GDPR) was introduced with effect from 25 May 2018. This is the second update members have had on the work undertaken to ensure the Council was compliant with the requirements of the act. This report seeks to update Members on actions taken since implementation and proposals to ensure the Council remains compliant going forward.

2. Recommendations

2.1 To receive the report and note the ongoing work to improve assurance of compliance with General Data Protection Regulations (GDPR).

3. Background

3.1 The General Data Protection Regulation (GDPR) was introduced with effect from 25 May 2018. This is the second update members have had on the work undertaken to ensure the Council was compliant with the requirements of the act. This report seeks to update Members on actions taken since implementation and proposals to ensure the Council remains compliant going forward and improves the level of assurance going forward.

3.2 At the time of the implementation of the GDPR, the principal piece of data protection legislation, the Data Protection Act, was amended and updated and is now the Data Protection Act 2018. When we refer to compliance with GDPR, this also encompasses compliance with the relevant provisions in the 2018 Act.

3.3 Both the Council and its individual Members are required to comply with the requirements, as data controllers. Member training was held in March 2018 and is part of new member induction in May 2019 and members have been provided with a copy of the privacy notice they should be using.

GDPR Implementation Guidance

The Council followed the guidance issued by the Information Commissioner when preparing for GDPR implementation which set out 12 steps:

4.1 **Awareness**

Senior Officers and Members should be made aware of the changes under GDPR so that impact and key areas can be identified and managed.

Senior officers have been kept informed throughout implementation and in subsequent months and this report will update Members in respect of steps taken.

GDPR has been discussed at Corporate Leadership Team and Extended Leadership Team to ensure senior officers are aware of the issues and that on-going compliance work is given a high profile.

Refresher training has recently been undertaken by all members of staff via an on-line module. Regular training will continue to be provided in the future. Initial training was given limited assurance as not all staff attended, this has since been resolved by the roll out of the on-line module and will be maintained via the system.

4.2 **Information you hold**

There is a need to undertake an information audit across the Council and have records of processing activities.

As mentioned above, the work to identify information held and to subsequently produce accurate and effective retention and disposal schedules is on-going. Whilst these had been attempted for the implementation of GDPR, these were not robust or sufficiently detailed for each service area. This was highlighted in the report and we are now using an audit tool to capture and maintain this information going forward. This approach will be more systematic and will ensure that data processors are maintaining their data sets effectively.

4.3 **Communicating privacy information**

Current privacy notes should be reviewed and a plan put in place for making any necessary changes.

All privacy notices were reviewed and refreshed as part of implementation of GDPR to ensure they met the new requirements. The council is currently digitising key processes and these all feature updated privacy notices.

4.4 **Individuals' rights**

Procedures should be checked and updated to ensure all the rights individuals have are included.

The Council's procedures were updated to include the new rights granted under GDPR alongside the pre-existing rights. These appear to be operating effectively without issues.

4.5 **Subject access requests**

Procedures should be updated to allow for the new rules:

- *generally information should be provided free of charge (there was a standard £10 charge)*

Information should be provided within one month (rather than 40 days)

If refusing a request for access, we must tell the person why and set out their rights to complain and to judicial remedy; again there is a time limit of one month to do this.

The Council's procedures were updated to take account of the changes and a central log is maintained of subject access requests. As previously, the Council does not receive a significant number of such requests. In the last 12 months 4 have been requested. 3 were responded to, however a fourth request was not released as it was requested on behalf of the subject and the subject did not give authority to release this information to the third party.

4.6 **Lawful basis for processing data**

The lawful basis for processing data must be identified, documented and set out on a privacy notice.

This information is included in each privacy notice. The new audit tool will enable this to be reviewed more systematically.

4.7 **Consent**

How we seek, record and manage consent should be reviewed and refreshed as necessary.

Where the Council relies on consent to process data (which is generally not the case), the consents have been reviewed and revised as necessary.

4.8 **Children**

GDPR brings in special protection for children's personal data and its use particularly for online services. The need for consent from either the child (if 16 or over) or the parent/guardian is explicit.

Whilst the Council does not generally process large amounts of children's data (unlike unitary or county councils) clearly some service areas, such as leisure, do process this data and work was undertaken to ensure the enhanced provisions under GDPR are complied with. The new audit tool will enable this to be reviewed more systematically.

4.9 **Data breaches**

Procedures should be in place to detect, report and investigate a personal data breach.

Only certain breaches have to be notified to the ICO; where it is likely to result in a risk to the rights and freedoms of individuals e.g. discrimination, damage to reputation, financial loss etc. These breaches have also been notified to the individual concerned.

The Council's procedure to deal with data breaches was revised to ensure compliance with GDPR requirements. Since GDPR implementation, the council has had one reportable breach. Although reported to the ICO, the ICO was content that the action taken by the Council was appropriate and no further action was deemed necessary by the ICO.

4.10 **Data Protection by Design and Data Protection Impact Assessments**

It will be a statutory requirement to adopt a privacy by design approach and to use Privacy Impact Assessments (or Data Protection Impact Assessments as they will be known) in certain circumstances.

The Council has adopted a privacy by design approach and this has been expanded under GDPR. Guidance on when and how a Data Protection Impact Assessment is needed is available. The audit tool mentioned above also contains useful guidance on when and how to undertake an assessment.

4.11 **Data Protection Officers**

It will be a statutory requirement to designate someone to take responsibility for data protection compliance, known as the Data Protection Officer (DPO).

The Assistant Director Democratic & Regulatory Services of South Staffordshire Council is currently designated as the DPO for the Council and works closely with the Head of Corporate Services to ensure Data Protection is managed effectively. This arrangement will be reviewed before the end of the financial year in line with the potential shared legal service.

4.12 **International**

There are provisions for those organisations operating in more than one EU state but these are not applicable to the Council.

GDPR Audits and other activity

5.1 An audit was undertaken by an External Auditor in April 2019 which highlighted a number of areas for improvement. Given the breadth and complexity of GDPR it was not unexpected that some issues would be raised by the audit. The audit highlighted some key areas of ongoing work that will need to be embedded to ensure ongoing compliance. The recommendations were agreed by senior management and the MetaCompliance audit tool mentioned above will assist in addressing a number of the issues raised which included ongoing training, awareness and recording of information assets and processing activity.

5.2 The Council's DPO has also undertaken a number of informal audits to ensure that, some 18 months on from implementation, all necessary procedures are in place and being used across the Council. This will be an on-going programme with different service teams being checked on a rolling programme. This not only gives assurance as to compliance but also serves to maintain awareness across the Council.

5.3 In order to ensure the Council is GDPR compliant, the following actions were also taken:

a) Contracts it has with 'data processors' i.e. external organisations who process personal data on behalf of the Council were reviewed and revised. Some residual contracts were highlighted in the GDPR audit and these have now been resolved.

b) Existing 'organisational' and 'technical' measures to ensure that personal data is kept 'safe' were reviewed and revised as necessary.

c) The incident management plan and procedures setting out when and how to notify the Commissioner and affected individuals if there was a breach of security i.e. unauthorised or unlawful processing, loss, damage or destruction of personal data were reviewed and revised as necessary.

Alternative Options	None the council must comply with these regulations, however the committee can choose not to receive ongoing reports.
Consultation	We have ongoing support from South Staffordshire District Council legal team regarding current advice and guidance.
Financial Implications	None; there are no further implications.
Contribution to the Delivery of the Strategic Plan	Data protection contributes to the sound running of the council.
Equality, Diversity and Human Rights Implications	None

Crime & Safety Issues	None

GDPR/Privacy Impact Assessment	Not required for this report.

	Risk Description	How We Manage It	Severity of Risk (RYG)
			State if risk is Red (severe), Yellow (material) or Green (tolerable) as determined by the Likelihood and Impact Assessment.
	Legal challenge if no process is in place	Ensure process is in place and regularly reviewed	Green
	Assurance of processes in place	Issues highlighted in the audits have been addressed	Green

Background documents

Relevant web links