East Lothian Council

REPORT TO: Cabinet

MEETING DATE: 12 June 2018

BY: Depute Chief Executive (Resources and People Services)

SUBJECT: Data Protection Policy

---

1 PURPOSE

1.1 On Friday, 25 May 2018, the European General Data Protection Regulation ('GDPR') came into effect. Accordingly, East Lothian Council's ('the Council') Data Protection Policy has been revised and updated in line with this change in legislation. This report requests the approval of the new Policy as appended (Appendix 1).

2 RECOMMENDATIONS

2.1 To approve the new Council Data Protection Policy.

3 BACKGROUND

3.1 GDPR introduces new obligations on the part of Data Controllers and Data Processors and enhances individual rights regarding data protection. The most significant changes to the Council's existing Data Protection Policy are summarised below.

3.2 **Data Protection Principles**: A new set of Data Protection Principles has been defined and includes an over-arching 'accountability principle' that requires Data Controllers such as the Council to evidence their compliance in detail.

3.3 **Special Category Data**: Previously called 'sensitive data' under the Data Protection Act 1998, Special Category Data requires enhanced protections. It has been redefined under GDPR, along with associated conditions for processing.

3.4 **Roles and responsibilities**: The Data Protection Officer is a new statutory role under the terms of GDPR, and roles and responsibilities have been updated accordingly. A new role of 'Information Champion' within Service areas has also been defined under the Policy, to ensure that best practice regarding data protection is implemented consistently across the Council.

3.5 **Rights of individuals**: Individual data subjects have new and enhanced rights under GDPR, including the right to request the erasure of their personal information, the right to restrict processing of their data, the right to data portability, and the enhanced right to be informed about how their information will be used.

3.6 **Data Protection by Design and Default**: In line with guidance from the national regulator, the UK Information Commissioner (ICO), the new Policy recognises the importance of integrating data protection into the Council's business processes from the start. It includes the conducting of Data Protection Impact Assessments (DPIAs) as a standard element within the Council's risk reporting and risk management frameworks.

3.7 **Data Breaches**: The revised Policy accounts for the new mandatory deadline of 72 hours to report relevant breaches to the ICO, and it mandates the formation of a new Data Breach Team within the Council to quickly and effectively assess and address data incidents. The Policy also notes the new maximum fine applicable to a security breach of £17,000,000 or 4% of turnover, whichever is higher.

4 POLICY IMPLICATIONS

4.1 This report requests the approval of the updated Council Data Protection Policy, which is applicable to all Council staff.

5 INTEGRATED IMPACT ASSESSMENT

5.1 The subject of this report has been through the Integrated Impact Assessment process and no negative impacts have been identified.

5.2 The Integrated Impact Assessment can be viewed online at: https://www.eastlothian.gov.uk/iiadpp.

6 RESOURCE IMPLICATIONS

6.1 Financial – there are no direct financial implications to this report.

6.2 Personnel – there are no new personnel implications to this report. The updated Policy requires the nomination of a statutory Data Protection Officer under the terms of GDPR, however this role was recruited in March 2018.

6.3 Other – there are no other resource implications to this report.

7 BACKGROUND PAPERS

7.1 Appendix 1 - Data Protection Policy

AUTHOR'S NAME	Zarya Rathé
DESIGNATION	Team Manager, Information Governance
CONTACT INFO	01620 827989; zrathe@eastlothian.gov.uk
DATE	29/05/2018

EAST LOTHIAN COUNCIL

Data Protection Policy

NB: This Policy is currently in draft, and has not yet been signed off by Cabinet.

East Lothian Council

CONTENTS

PAGE

Document Control		
Version	**Date**	**Description**
1.0	17/04/2012	First approved version
2.0	12/07/2012	Second approved version
3.0	07/05/2018	Re-drafted in line with the General Data Protection Regulation (GDPR) / Data Protection Act 2018.
3.1	29/05/2018	Maximum fine applicable to a security breach (section 16) amended from €20,000,000 to £17,000,000 in line with ICO guidance.
3.2	29/05/2018	Minor proofreading updates.

1. Introduction

1.1. This document sets out East Lothian Council's policy regarding data protection. To perform its public function and operate efficiently, East Lothian Council ('the Council') must collect and use information about individuals. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of government.

1.2. The Council regards respect for the privacy of individuals and the lawful and careful treatment of personal information as essential to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. To this end, the Council is committed to protecting the rights and privacy of individuals including those rights set out in the General Data Protection Regulation ('GDPR'), Data Protection Act 2018 ('DPA 2018') and other data protection legislation.

1.3. The Council is fully committed to data protection compliance and will follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, volunteers and any other partners of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and comply with their duties and responsibilities under GDPR and the DPA 2018.

1.4. GDPR came into force on 25 May 2018, with DPA 2018 enacted shortly thereafter. The Council's principal aim is to ensure that all personal data processing carried out by the Council, or on its behalf, complies with the six data protection principles and other key legislative requirements.

2. Statement of Intent

2.1. East Lothian Council regards the lawful and correct treatment of personal data as very important to successful operations, and to maintaining confidence between those with whom it deals, both internally and externally.

2.2. East Lothian Council recognises the importance of ensuring that the Council treats personal data lawfully and correctly and the Council fully endorses and adheres to the principles of data protection detailed in the DPA 2018. Any employee found to be breaching the terms and conditions of this policy may be subject to disciplinary procedures.

3. Definitions

3.1. **Personal data:** information which relates to a living individual who can be identified either directly or indirectly from that information or any other information likely to come into the possession of the data controller. This includes any expressions of opinion and any indications of the intentions of the data controller, or any other person, in respect of the individual.

3.2 **Special category data:** personal data consisting of information revealing any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex life.
- Sexual orientation.

Special category data has enhanced protections for processing compared with personal data.

3.3. **Record**: 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.

3.4 **Processing**: any action performed on personal data, including (but not limited to) collecting, storing, sharing, destroying or preserving data.

3.5 **Data controller**: a person or organisation who decides how personal information can be processed, and for what purposes. East Lothian Council is a data controller.

3.6. **Data processor:** a person or organisation (other than an employee of the data controller) who processes personal data on behalf of a data controller.

3.7. **Data subject:** an individual about whom the Council holds personal data.

4. Roles and responsibilities

4.1 **Senior Information Risk Owner (SIRO):** the SIRO has overall strategic responsibility for governance in relation to data protection risks. The SIRO:

- Acts as advocate for information risk at the Corporate Management Team (CMT);
- Provides written advice to the Chief Finance Officer for the Annual Governance Statement relating to information risk;
- Drives cultural change regarding information risks in a realistic and effective manner;
- Oversees the reporting and management of information incidents;
- In liaison with the Chief Executive and the Depute Chiefs, ensures the Information Asset Owner and Information Asset Administrator roles are in place to support the SIRO role.

The Council's SIRO is the Head of Council Resources.

4.2 **Data Protection Officer (DPO):** the DPO is a statutory role under GDPR. The DPO:

- Informs and advises the Council and its employees about their obligations to comply with the GDPR and DPA 2018;
- Monitors compliance with the GDPR and DPA 2018, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations and related audits;
- Provides advice about data protection impact assessments and monitors their performance;
- Co-operates with the supervisory authority (the Information Commissioner's Office);
- Acts as the contact point for the Information Commissioner's Office and members of the public on issues related to the processing of personal data.

The Council's DPO is the Team Manager – Information Governance.

4.3 **IT Team Manager - Infrastructure and Security:** the IT Team Manager - Infrastructure and Security is responsible for creating, implementing and maintaining the Council's Information Security Policy and procedures to reflect changing local and national requirements. This includes requirements arising from legislation, security standards and national guidance.

The IT Team Manager - Infrastructure and Security supports Service areas in achieving best practice and compliance with security requirements.

4.4 **Information Champions:** Information Champions ensure that best practice regarding information governance and security is implemented consistently across the Council by acting as the main points of contact within Services for Information Governance issues. They liaise with the Team Manager - Information Governance / Data Protection Officer and the IT Team Manager - Infrastructure and Security to discuss changes to policies/procedures, disseminate information and troubleshoot problems.

Information Champions are nominated by Service Managers.

4.5 **Individual members of staff and elected members:** Individual members of staff and elected members are responsible for protecting personal information held or processed on computer, or held in paper records, within their care.

5. Notification

5.1. Data controllers are required to notify the Information Commissioner of the processing that they undertake.

5.2. The Council will maintain its register entry and annually review its processing to ensure that its register entry is accurate and up to date.

6. The Data Protection Principles

The data protection principles set out the main responsibilities for organisations. They stipulate that personal data shall be:

a) processed lawfully, fairly and in a transparent manner;
b) collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date:
e) kept no longer than is necessary for that purpose or those purposes;
f) processed in a manner that 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;

In addition to the six principles listed above, the data controller shall be responsible for, and be able to demonstrate, compliance with the principles (also known as the 'accountability principle').

7. Rights of individuals: The GDPR provides individuals with the following rights regarding their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information.
- The right to rectification, which is the right to require the Council to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Council processing their personal information.
- Rights in relation to automated decision making and profiling.

The Council publishes detailed information for the public that sets out what these rights are and how these can be exercised.

8. Compliance with the Principles

East Lothian Council will, through appropriate application of criteria and controls:

- ensure the fair collection and use of information through the use of Privacy Notices;
- meet its legal obligations to specify the purposes for which information is used; including specific requirements that must be met to ensure fair and lawful sharing of personal data both internally and externally;
- collect and process appropriate information only to the extent that is needed to fulfill operational needs or to comply with any legal requirement;
- ensure the accuracy of information used;
- implement procedures to restrict the length of time information is held, including implementation of a corporate records Retention Schedule;

- ensure that people about whom information is held are able to fully exercise their rights under the Act, as listed in Section 7 of this Policy;
- ensure compliance with the East Lothian Council IT Policies/ Information Security Polices to safeguard personal data;
- ensure that information is not transferred abroad without suitable safeguards.

9. Information Handling and Collection (Principles a, b and c)

9.1. East Lothian Council will process all personal data for the purpose of providing an effective delivery of service in accordance with the aims, responsibilities and obligations of the Council.

9.2. All personal data will be processed in accordance with Privacy Notices issued to individuals by the relevant Council Service at the point of data collection. These Privacy Notices will inform data subjects of:

- The name and contact details of the Council;
- The name and contact details of the Council's Data Protection Officer;
- The purposes for processing their personal data;
- The lawful basis for processing their personal data, including conditions regarding 'sensitive processing', such as the lawful basis for processing special category data;
- The categories of personal data obtained;
- The recipients or categories of recipients of the personal data, including details of any transfers to third countries or international organisations;
- The retention periods for the personal data;
- The rights available to data subjects;
- The details of the existence of automated decision-making, including profiling.

Privacy Notices will provide this information in a way that is concise, transparent, easily accessible and using clear and plain language.

9.3. Personal data will only be collected where there is a specific purpose for doing so. It will not be used for any other purpose except where allowed by the GDPR, DPA 2018 or required by law. The personal data collected shall be limited to what is necessary in relation to that specific purpose.

10. Records Management (Principles d and e)

10.1. The Council will implement procedures to ensure that all personal data it holds are accurate in respect of matters of fact and, where necessary, kept up to date.

10.2. Opinions of officers of the Council that are recorded will be carefully and professionally expressed. When processing personal data relating to criminal offences, Council officers will distinguish between matters of fact and matters of personal assessment or opinion.

10.3. The Council will not hold personal data for longer than is reasonably required. The Council will comply with its corporate Retention Schedule.

10.4. Further information about records management and records retention can be found in East Lothian Council's Records Management Plan.

11. Security (Principle f)

10.1. East Lothian Council will ensure that there is someone with specific responsibility for data security. Currently, the IT Manager - Infrastructure and Security has this responsibility.

10.2. All officers of the Council are responsible for ensuring that personal data are held securely at all times.

10.3. Access to all Council systems is password protected and only authorised personnel have access.

10.4. Personal data will be safely and responsibly destroyed when they are no longer required.

10.5 Personal data will be held in official recordkeeping systems with appropriate records management controls in place, in line with the Council's Records Management Plan.

10.5. All officers of the Council and individuals undertaking work for the Council will adhere to the Council's IT security policies and procedures.

12. Accountability principle

12.1. All officers of the Council and individuals undertaking work for the Council have a personal responsibility to ensure the secure and compliant processing of personal data.

12.2. Roles with specific data protection responsibilities are listed in Section 4 of this Policy.

12.3 A record of data processing activities will be maintained by the Council in an Information Asset Register, which will identify the members of staff responsible for overseeing compliance for each processing activity (Information Asset Owners).

12.4 All Heads of Service and Service Managers will ensure that documentation evidencing the Council's compliance with GDPR / DPA 2018 remains accessible and up-to-date within official recordkeeping systems.

13. Data protection by design and default

13.1 The Council recognises the importance of integrating data protection into its business processes from the start. Accordingly, the Council will conduct a Data Protection Impact Assessment (DPIA) as part of any new data processing activity.

13.2 DPIAs will be included as a standard element within the Council's risk reporting and risk management frameworks.

13.3 The Council will integrate data protection with reference to the 7 Foundational Principles of Privacy by Design:

1) **Proactive, not reactive:** anticipating and preventing privacy invasive events before they happen.
2) **Privacy as default:** personal data are automatically protected in any business practice or IT system. No action is required on the part of the individual to protect their privacy.
3) **Privacy embedded into design:** privacy of personal data is embedded into the design and architecture of IT systems and business practices. Privacy is integral to the core functionality of the system.
4) **Full functionality:** activities regarding privacy seek to accommodate all legitimate interests and objectives in a win-win approach.
5) **End-to-end security:** data protection extends security throughout the entire lifecycle of the data involved.
6) **Visibility and transparency**: all stakeholders are assured that business practices or technology operate according to

stated promises and objectives, subject to independent verification.

7) **Respect for user privacy**: adopt a user-centric approach which uses strong privacy defaults, appropriate notice and empowering user-friendly options.

14. Disclosures

14.1. East Lothian Council reserves the right to disclose information under certain circumstances where allowed by law.

14.2. When a request for disclosure is made, the Council will consider each request individually and where a disclosure is justified, the Council will only disclose the minimum data required.

14.3. In order to improve service delivery and to meet its responsibilities, the Council may enter into data sharing agreements with other organisations where data sharing is allowed by law. Where this is the case, the Council will ensure that an Information Sharing Agreement with that organisation is in place which ensures the data sharing is in compliance with the law and this policy.

15. Elected Members and Data Protection

15.1. Where Elected Members work on behalf of the Council, this policy applies to them, and they must abide by all associated procedures. Should any breach of the DPA occur, it will be the Council's responsibility.

15.2. Where Elected Members work for their constituents, they are data controllers in their own right and must register with the Information Commissioner. Should any breach of the DPA occur, it will be the Elected Member's responsibility.

16. Complaints, Enforcement and Dealing with Breaches

16.1. All complaints regarding data protection should be made to the Council's Data Protection Officer at dpo@eastlothian.gov.uk.

16.2 The maximum fine for data protection breaches is £17,000,000 or 4% of turnover (whichever is higher), with a mandatory deadline of 72 hours to report relevant breaches to the UK Information Commissioner. Therefore, the Data Breach Team should immediately be informed of any suspected internal breaches of the GDPR / DPA 2018, as laid out in the Council's Data Breach Procedure.

16.3. All Council staff, contractors and elected members will co-operate fully with any investigation into an alleged breach of the GDPR / DPA 2018 undertaken by the Council's Data Breach Team or the Information Commissioner.

16.4. The Data Breach Team will apply a fair and consistent approach to the recording and management of all data protection breaches, including notification of breaches to affected individuals where necessary. In each case, this will include a risk assessment of the consequences of the breach, conducted in line with the relevant guidance from the Information Commissioner's Office and up to date case law. Precedent within the Council will also be taken into account.

16.5 Depending on the nature of the breach, breaches of the GDPR / DPA 2018 or of this policy may result in disciplinary proceedings for the staff involved.

17. Managing Data Protection

17.1. East Lothian Council will ensure that-

- the Data Protection Officer will provide advice on data protection compliance to all officers processing personal data within Council;
- Heads of Service and Service Managers will ensure that all staff have access to this Policy and that they receive relevant training;
- training for all staff will be made available via e-learning, online and printed guidance, supplemented by person-to-person training where required;
- everyone managing and handling personal data understands that they are responsible for following good data protection practice;
- everyone managing and handling personal data is appropriately trained to do so and has the opportunity to receive training;
- everyone managing and handling personal data is appropriately supervised;
- queries about managing and handling personal data are promptly and courteously dealt with;
- methods of managing and handling personal data are regularly assessed and evaluated;
- performance of managing and handling personal data is regularly assessed and evaluated;
- Risks regarding data protection are regularly reported at a senior level, with appropriate mitigating actions taken.

18. Related Policies and Procedures

- GDPR Toolkit
- Data Breach Procedure
- IT Acceptable Use Policy
- Information and Records Management Policy
- East Lothian Council Records Management Plan
- East Lothian Council Retention Schedule
- E-learning module: General Data Protection Regulation

19. Contact Information

18.1. East Lothian Council's Data Protection Officer can be contacted at:

Data Protection Officer
Licensing, Administration and Democratic Services
John Muir House
Haddington
dpo@eastlothian.gov.uk
Tel. 01620 82 7989