Elmbridge Borough Council Data Protection Policy

October 2020

Elmbridge
Borough Council
... bridging the communities ...

Contents

Policy Statement

1. Policy

Elmbridge Borough Council (the Council) collects and uses personal data in order to carry out its business and provide services. This Data Protection Policy sets out how the Council will protect individuals' rights in relation to the storage, access, use and disclosure of their personal data, and defines standards to achieve compliance with current legislation.

The Data Protection Act 2018 and General Data Protection Regulation (GDPR) detail requirements that must be complied with to ensure that the rights and freedoms of living individuals are not compromised, and that all personal data is processed in a secure and appropriate manner. The legislation also stipulates that those who record and use personal information must be open about how the information is used and must follow good handling practices. This applies to the whole lifecycle of information, including the collection, use, disclosure, retention and destruction of data. the Council is committed to fulfilling its obligations under this data protection legislation and has produced this policy to both assist officers and provide assurance to its customers.

2. Purpose

The purpose of this policy is to enable the Council to:

- Comply with all legislation in respect of the personal data it holds about individuals
- Protect the Council's clients, service users, staff and other individuals for whom the Council deals with in order to conduct its business or provide services
- Follow good practice. This policy is a key document within the Council's Information Governance Framework which provides a formal structure for the implementation of the requirements of GDPR and the Data Protection Act 201

3. Scope

This policy applies to all the personal data held by the Council and includes manual/paper records, and personal data that is electronically processed by a computer or any other means. This policy applies to anyone accessing or using all Council personal data held by the Council in any form. It applies to all Departments, Committees, Partners, contractual third parties and agents of the Council including:

- Customers
- Current, past and prospective employees
- Contractors
- Councillors
- Suppliers
- Service Users
- Carers
- Residents
- Others with whom the Council communicates

4. Applying the Policy

4.1 What is Personal Data

Under GDPR Personal data refers to any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- A name
- An identification number
- Location data
- Online identifier
- Physical details
- Physiological details
- Genetic details
- Mental health
- Economic factors
- Cultural or social identity of natural persons

4.2 Special Category Data (Sensitive Personal Data)

The following categories of personal data relate to more private matters of a data subject's life:

- Racial or Ethnic origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical or mental health
- Sexual orientation or sex life
- Criminal proceeding or convictions
- Genetic data
- Biometric data

4.3 Data Protection Principles

There are 6 key definitions in the GDPR. These principles do not provide hard and fast rules but embody the spirit of the general data protection regime. Compliance with these principles is fundamental to embedding good data protection and is key to the Council compliance with the provisions of GDPR.

General Data Protection Regulation Principles

- **Lawfulness, fairness and transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- **Purpose - purpose limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- **Data minimisation** - Personal Data shall be adequate, relevant, and limited only to what is necessary in relation to the purposes for which it is processed
- **Accuracy** - Personal Data shall be accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified.
- **Storage limitation** - Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods in so far as the said personal data will be processed only for
    - archiving purposes
    - in the public interest
    - scientific or historical research purposes
- **Integrity and confidentiality** - Personal data shall be processed in a manner that ensures appropriate security, including protection against accidental loss, destruction or damage.
- **Accountability Principle** - The controller the Council shall be responsible for and be able to demonstrate compliance with all the above principles
- **Overseas Transfer of Personal Data** - Data should not be transferred to other countries that do not have the same level of data protection Although this is not considered one of the GDPR principles GDPR does require that organisations

must receive explicit consent from their Data Subjects for their personal information to be transferred outside of the EEA.

Based upon the GDPR principles, the Council will:

- Observe fully, conditions regarding the fair collection and use of personal information
- Meet its obligations to specify the purpose for which information is used
- Collect and process appropriate information, to the extent for which it is needed, to fulfil operational needs, or to comply with any legal requirements
- Apply checks to determine the length of time that information is held
- Take all appropriate security measures to safeguard personal information
- Ensure the rights of data subjects, about whom information is held, are fully exercised
- Ensure that all staff managing and handling personal information understand their contractual responsibilities
- Ensure that all staff managing and handling personal information are appropriately trained
- Ensure that all staff managing and handling personal information are appropriately supervised
- Ensure that methods of handling personal information are regularly reviewed and evaluated
- Ensure that personal information is not transferred abroad without the appropriate safeguards.

4.4 Personal Information Sharing

Any regular sharing of personal information between the Council and other agencies will be subject to an information sharing protocol, and an agreed data transfer process that meets the requirements of the Data Protection Act. Personal information sharing with the Council must comply with the Data protection principles of ‘Purpose’ stating that personal data shall be obtained only for one or more specified or lawful purposes and shall not be processed in a manner incompatible with that purpose.

4.5 Data Privacy Impact Assessments (DPIA)

DPIAs are now mandatory under GDPR. A DPIA must be carried out for processing that is likely to result in a high risk to individuals. It is also good practice to carry out a DPIA for any major project that requires the processing of personal data. A DPIA must:

- Describe the nature, scope, context and purpose of the processing
- Assess necessity

- Identify and assess risks to individuals
- Identify additional, measures to mitigate risks

The results of DPIAs should be reported either to the DPO or the Information Governance Group where any high risks are identified.

4.6 Consent

GDPR sets a high standard for consent as a lawful basis for processing personal or special category data. Where processing is based on consent, the Council is required to demonstrate that the Data Subject has consented to the processing of their personal data. Consent therefore requires either a positive opt-in process or a clearly written declaration, pre-ticked boxes or any other method of default approval cannot be used. The Data Subject has the right to withdraw their consent at any time where consent is the basis for processing personal data.

4.7 Data Subjects' Rights and Subject Access Requests (SARs)

Data Subjects whose data is held by the Council have the following rights over their personal data and can access that data and any supplementary information about how their data is being processed, by Subject Access request:

- The right to be informed about how and why their personal data is processed
- The right to access their data
- The right to rectify their data
- The right to be forgotten – erasure of their data
- The right to restrict processing of their data
- The right to data portability
- The right to object to processing of their data
- The right to object to profiling, or automated decision making

These requests must be handled and responded to in a timely manner in line with the requirements of GDPR which determines that all SARs must be:

- Provided free of charge
- Answered without delay and within 30 days.

All SARs will be managed and tracked by the Data Protection Officer.

4.8 Training

Data Protection training will be made available for all the Council Employees. Training will be mandatory for all staff who process personal or sensitive data. The training provided is aimed to ensure that all individuals understand their responsibilities for managing data in line with all new legislation. Training materials

must be kept up to date with all relevant UK and EU legislation and should be made available to all staff.

5. Roles and Responsibilities

5.1 Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility and accountability in all aspects of Data Protection. They are required to provide assurance that all risks are effectively managed and mitigated. They will delegate compliance of this Data Protection and other related policies to the Data Protection Officer.

5.2 Data Protection Officer (DPO)

The DPOs role is:

- To inform and advise the Council and its employees about the Council's obligations to comply with GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, along with the Council's policies in relation to the protection of personal data, including the assignment of responsibilities, awareness training and training of staff involved in processing operations and conducting related audits
- Provide advice and monitor data impact assessments (DPIA)
- Co-operate with the Supervisory Authority – The ICO
- To be the first point of contact for the supervisory authorities and for individuals on issues relating to processing, including prior consultation where appropriate
- Perform their duties in an independent manner with due regard to the risk associated with processing of operations, considering the nature, scope, context and purposes of all data processing
- Escalate where appropriate to the CMB.

5.3 Information Asset Owners (IAOs)

IAOs take responsibility for:

- Ensuring the correct protection and handling arrangements for the information assets that they own
- Ensuring that the Council Information Governance Policies are communicated and implemented within their respective areas of responsibility, and for ensuring that any issues regarding resourcing, training, and compliance are escalated to the DPO and or the IGG

- Responsible for ensuring that staff are informed of any updated changes to Information Governance Policies.

5.4 Information Asset Administrators (IAAs)

IAAs take responsibility for:

- Keeping the Asset Registers up to date
- Ensuring information handling procedures are managed
- Ensuring that personal information is not unlawfully exploited
- Acting as first port of call for any staff seeking advice related to data protection

5.5 Individual Employees

All staff whether permanent or temporary are required to:

- Read and understand and accept any policies and procedures that relate to personal data that they may handle as part of their role
- Take responsibility for data protection and adhere to this policy and related procedures Attend training related to Data Protection or the handling of personal data;
- Understand the main concepts of Data Protection related legislation
- Identify and report any risks that they identify in relations to the security of personal data to their line manager
- Assist their customers to understand their rights and the Council's responsibilities regarding Data Protection
- Identify any SARs and follow the correct reporting procedure and escalation

6. Governance

6.1 Council Management Board (CMB)

CMB should

- maintain oversight of the Information Governance Group (IGG)
- ensure that the Council's approach is effective in terms of resources, commitment and execution of all matters related to Information Governance.
- review and provide final approval for all Information Governance related policies

6.2 The Information Governance Group (IGG)

The IGG is Chaired by the Head of ICT and Digital Services and will meet once every two months. It is the role of the IGG to:

- Decide and/or recommend operational matters around all aspects of Information Governance
- Establish a Framework to embed best practice in all aspects of Information Governance
- Define the organisational policies in respect of data protection considering any legal and local authority requirements
- Provide regular reporting to the CMB which should include any key risks relating to the Council's ability to demonstrate compliance to regulation/policies
- Provide an update on reported incidents of Personal Data Breaches, SARs, IGG actions, audit points and any other key points as agreed by the IGG members

6.3 Monitoring Compliance

Compliance with this policy and related standards will be monitored by the DPO and IGG. Ongoing monitoring and an action plan for improvements will be formulated by the IGG and communicated accordingly. Any disregard for this policy may be treated as misconduct and a serious breach may be treated as gross misconduct and will be subject to the Council's disciplinary procedure. If you do not understand the implications of this policy or how it may apply to you, seek advice from your manager, the Data Protection Officer, any member of the legal team, or any member of the IGG.

6.4 Review and Revision

This policy will be reviewed as it is deemed appropriate, but in line with any new or changed legislation, regulations or business practices but no less frequently than every 12 months. Policy review will be undertaken by the Information Governance Group and presented to the CMB for approval.

7. References

Internal guidance on implementation of the Data Protection Act, and key Data Protection Act related documents are available to Council employees via the Information Governance pages on Bridge-it. General guidance and a free helpdesk dealing with GDPR related issues are available to Council employees and the public via the Internet on the Information Commissioner's Office website.

Registration Number Z4771967

The Data Protection Act can be accessed on the Internet via the UK legislation database at: the Government Legislation portal.

The Data Protection Officer for Elmbridge Borough Council can be contacted on 01372 474149 or by e-mail at dataprotection@elmbridge.gov.uk.