



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

Data Protection Policy

November 2016

Document Control

Organisation	Elmbridge Borough Council
Title	Data Protection Policy
Author	Chair of Information Governance Group
Owner	Information Governance Group
Subject	Data Protection
Protective Marking	Not protectively marked
Review date	April 2018

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
November 2016	Anna Grealis	EBC Data Protection Policy April 2012	Minor changes to section numbering. Change to web details for access on Intranet to internal DP advice and guidance in section 12 Changes to wording in paragraphs 1, 2, 5.1, 8.4, 8.5 and 8.6.1 for clarification purposes
August 2017	Anna Grealis	EBC Data Protection Policy April 2016	Update to ICO website link

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Contents

- 1 Policy Statement
- 2 Purpose
- 3 Scope
- 4 Risks
- 5 Applying the policy
- 6 Policy Governance
- 7 Review and Revision
- 8 References

1. Policy Statement

Elmbridge Borough Council will ensure that every user, as defined below, is aware of, and understands, their responsibilities under the Data Protection Act 1998 and other relevant legislation.

This policy outlines the responsibilities of all users, which are Employees, Senior Management, Councillors, Volunteers, those undertaking work experience, all network users and third party Contractors under the Data Protection Act 1998.

2. Purpose

Elmbridge Borough Council collects, holds and uses data about people (Data Subjects) with whom it deals with in order to conduct its business or to provide services. This data covers, but is not restricted to, the following:

- Customers.
- Current, past and prospective employees.
- Councillors.
- Suppliers.
- Residents.
- Others with whom the Council communicates.

3. Scope

Any information must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer, or recorded on other media. There are safeguards in the Data Protection Act 1998 to ensure that personal information is securely dealt with and handled correctly.

This policy relates to all personal data held by Elmbridge Borough Council in any form. It applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to information held or processed by Elmbridge Borough Council.

Elmbridge Borough Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998, and other relevant information security legislation. Therefore, the Council will ensure that all Councillors, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to any information held by or on behalf of the Council are fully aware of, and abide by, their duties and responsibilities under this legislation.

4. Risks

Elmbridge Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- inadequate records management
- inaccurate and inadequate data
- Inadvertent or deliberate disclosure of personal data in breach of the Act

- commission of any criminal offence by unauthorised access to or disclosure of personal data
- reputational risk
- financial risk in the event of enforcement action by the Information Commissioner

5. Applying the Policy

5.1 Relevant Legislation

The following statutory legislation governs aspects of the Council's data protection arrangements. This list is not exhaustive:

Legislation	Areas Covered
The Human Rights Act 1998	Right to respect for private and family life, his home and his correspondence (Article 8)
The Data Protection Act 1998	Framework of rights and duties which are designed to safeguard personal data.

The Data Protection Act 1998 provides a framework which balances the legitimate needs of organisations to collect and use personal data for businesses and other purposes against the right of individuals to respect for the privacy of their personal details.

The data protection principles must be complied with when dealing with personal data. Records must be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

5.2 What is Personal Data?

Personal data is defined in the 1998 Act as:

“data which relate to a living individual who can be identified:

- a) from those data; or,*
- b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller;*

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.”

8.3 What are the Principles of Data Protection?

The Data Protection Act 1998 stipulates that anyone processing personal data must comply with **Eight Principles** of data protection. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;

2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Shall be kept secure - i.e. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Data Protection Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data. Sensitive personal data is defined as:

“personal data consisting of information as to:

- a) the racial or ethnic origin of the data subject,*
- b) his political opinions,*
- c) his religious beliefs or other beliefs of a similar nature,*
- d) whether he is a member of a trade union,*
- e) his physical or mental health or condition,*
- f) his sexual life,*
- g) the commission or alleged commission by him of any offence, or*
- h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.¹”*

8.4 The Rights of Individuals including Access to Personal Data

Individuals whose data is held by Elmbridge Borough Council have the following rights:

- the right of access to a copy of the information comprised in their personal data,
- the right to prevent processing likely to cause damage or distress,
- the right in certain circumstances to have inaccurate data rectified, blocked, erased or destroyed.
- the right to claim compensation for damages caused by a breach of the Act.

There are exemptions to the right of subject access and so some personal data cannot be obtained by making a subject access request. In cases where no exemption applies Elmbridge Borough Council will respond to valid subject access requests promptly and in any event within 40 days of receiving the request. A £10 fee is payable and requests must be made in writing. This fee is sometimes waived if it is felt that the administration of dealing with the fee is disproportionate to the subject access request.

8.5 How will Elmbridge Borough Council ensure Compliance?

In order to ensure it meets its obligations under the Data Protection Act, Elmbridge Borough Council will ensure that:

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained.
- Everyone managing and handling personal information is appropriately supervised.
- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.
- Queries about handling personal information are promptly and courteously dealt with.

Elmbridge Borough Council will, through appropriate management and the use of strict criteria and controls:

- Observe fully the conditions regarding the fair collection and use of personal information.
- Meet its obligations to specify the purpose(s) for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality and accuracy of information used.
- Apply strict checks to determine the length of time information is held to ensure it is not kept for longer than necessary.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of Data Subjects can be fully exercised under the Data Protection Act.

8.6 What Roles and Responsibilities have been Assigned?

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are as follows :

8.6.1 Data Protection Officer and the legal team

The Head of Legal Services is the Data Protection Officer. The legal team along with the Information Governance Group will promote this policy and provide advice to departments to facilitate the correct processing of Requests for Access and other Data Protection related issues. They will also monitor departments to ensure compliance with statutory and regulatory obligations. The Data Protection Officer will hold a central record of subject access requests received and the responses to these requests, It is the responsibility of the Heads of Service to update this central record, which is accessible, with details of subject access requests, .

8.6.2 Corporate Management Board (CMB)

CMB will provide support and approval for this Data Protection Policy and any related initiatives across the Council.

8.6.3 The Information Governance Group (IGG)

The IGG will meet regularly to review information management across the Council. As part of this they will address any Data Protection related issues that arise and generate initiatives or communications as necessary to ensure compliance with the Elmbridge Borough Council Data Protection Policy. The Chair of the IGG will liaise with the Data Protection Officer and the legal team as required.

8.6.4 Managers

Managers are responsible for ensuring that the Elmbridge Borough Council Data Protection Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing, training and compliance concerns are communicated back to the Data Protection Officer and/or the IGG in a timely manner.

8.6.5 Individual Employees

Individual employees will be responsible for attending training and indicating their understanding of this Data Protection Policy and ensuring that Subject Access Requests and other Data Protection related issues in their team are handled in compliance with this policy.

9. Policy Compliance

If any user is found to have breached this policy, they will be subject to Elmbridge Borough Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

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.

10. Policy Governance

The following table identifies who within Elmbridge Borough Council is Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Information Governance Group
Consulted	CMB
Informed	All

11. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Information Governance Group.

12. References

Elmbridge Borough Council Data Protection Policy November 2016

Internal guidance on implementation of the Data Protection Act, and key Data Protection Act related documents are available to Council employees via Bridge-It, search for 'Data Protection'.

General guidance and a free helpdesk dealing with Data Protection Act related issues are available to Council employees and the public via the Internet on the Information Commissioner's website at:

<https://ico.org.uk/>

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

<http://www.legislation.gov.uk/ukpga/1998/29/contents>

The Data Protection Officer for Elmbridge Borough Council can be contacted on 01372 474192 or by e-mail at aharrison@elmbridge.gov.uk