Cheltenham Borough Council Data Protection Policy

Version control

Document name: Data Protection Policy

Version: 1.0

Responsible officer

- Claire Hughes, Corporate Director and Monitoring Officer

Approved by: Cabinet

Next review date: May 2025

Retention period: Delete one year after new version

Revision history

Revision date	Version	Description
May 2023	1	New Policy

Consultees

Internal

- Corporate Governance Group and Leadership Team

External

- N/A

Distribution

All Staff and Council Website

Contents

1. Introduction

1.1. The purpose of this policy is to ensure that Cheltenham Borough Council (the Council) and individuals working for, or on its behalf, are aware of their obligations under, and comply with, UK Data Protection Law.

1.2. The Council collects and processes different types of information about the people with whom it deals and communicates with in order to provide its services to the community.

1.3. It is the Council's obligation, as the Data Controller, to ensure compliance with UK Data Protection Law.

1.4. The following policy outlines the Council's responsibilities and processes surrounding the personal data which is processed by the Council and its employees.

2. Scope

2.1. This policy applies to:

- all forms of information and data owned, administered, stored, archived or controlled by the Council, including electronic and hard copy formats;
- information and data in test, training and live environments, however it is hosted;
- all elected members and staff of the Council including temporary and contract staff, volunteers and third parties accessing or using the Council's information, data and/or network;
- all electronic and communication devices owned, administered, controlled or sanctioned for use by the Council; and
- all Service users and members of the public whose personal information is held by the Council in order to provide its services.

3. Policy Statement

3.1. The Council is required to collect and use personal and/or sensitive information about people in order to operate. This includes information about;

- members of the public, service users, clients and customers;
- current, past and prospective employees; and
- suppliers and other third parties.

3.2. In addition, the authority may have to collect and use information in order to comply with the legal requirements of central government. This personal information must also be handled in line with the law

3.3. Therefore, the Council is committed to:

- complying with both law and good practice;
- respecting individuals' rights;
- being open and honest with individuals whose data is collected and held;
- providing training and support for staff who handle personal data, so that they can act confidently and consistently;
- ensure retention & disposal of personal information is adhered to;
- Implement appropriate technical and organisational security measures to safeguard personal information are in place;
- ensure personal information is not transferred abroad without suitable safeguards or adequate protection; and
- ensure the quality of information used by the Council.

3.4. To this end the Council will only process personal or special category data where an appropriate legal basis can be identified.

3.5. The lawful basis for processing are set out in Article 6 of the UK General Data Protection Regulation (UK GDPR). At least one of these must apply whenever the Council is processing personal data. Click here for full details of the Lawful Basis for processing

3.6. Further conditions are available within the Data Protection Act 2018, for help and advice in determining the appropriate condition contact: Data.Protection@cheltenham.gov.uk

3.7. Where the Council is processing personal data it fully endorses and follows the principles of UK GDPR outlined below.

3.8. Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered as being incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and
- 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. Furthermore, the Council is responsible for, and must be able to demonstrate compliance with the 6 principles above ('accountability').

4. Duties and Responsibilities

4.1. The Council is registered as a Data Controller. It is responsible for the fair and lawful processing of personal and/or sensitive personal information, this rests with the Chief Executive on behalf of Council as a whole.

4.2. However, it is the responsibility of all employees and elected members to handle information and data correctly. As an individual representing, working for, or on behalf of, the Council it is essential that you:

- follow Corporate and/or departmental policy, procedures and guidance on the collection and use of personal/special information and data;
- handle all personal information in accordance with the Council's security policies and procedures; be clear why you are using personal/special information;
- tell people why their information is being collected, what it will be used for and how it will be managed from collection to destruction;
- collect only the minimum amount of personal/special data needed, and use it only for the purposes specified or in line with legal requirements;
- only access the personal/special data that you require to carry out your role and no more;
- ensure the personal/special information is input correctly and accurately;
- if you receive a request from an individual for information held by the Council about them you should email it to: Data.Protection@cheltenham.gov.uk
- understand and undertake the mandatory training relating to Information Security and Data Protection within two weeks of starting in post and in a timely manner when renewing annual training.

4.3. The Council will ensure that;

- employee and member training needs are identified, and training provided to ensure that those managing and handling personal/sensitive information understand their responsibilities and follow good practice; and
- anyone who makes a request regarding their personal information to the Council is responded to.

5. Data Subject Rights

5.1. The UK GDPR outlines several data subject rights and the Council will ensure that the rights of people about whom information is held can be fully exercised. The rights are as follows:

a) The right to be informed Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

b) The right of access (also known as Subject Access Requests) Under the UK GDPR, individuals will have the right to obtain:
   - confirmation that their data is being processed;
   - access to their personal data; and
   - other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

This Council must provide a copy of the information free of charge. However, a 'reasonable fee' can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt.

This can be extended by a further two months where requests are complex or numerous. If this is the case, the Council must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Council can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where the Council refuses to respond to a request, it must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

The Council must verify the identity of the person making the request, using “reasonable means”. If the request is made electronically, the Council should provide the information in a commonly used electronic format.

If you receive a subject access request, please contact Data.Protection@cheltenham.gov.uk

c) The right to rectification - Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.
   - An individual can make a request for rectification verbally or in writing.
   - The Council has one calendar month to respond to a request.
   - In certain circumstances you can refuse a request for rectification. Contact the Data Protection Officer should you receive a request of this nature.

d) The right to erasure - Individuals have a right to have personal data erased. The right to erasure is also known as ‘the right to be forgotten’.
   - Individuals can make a request for erasure verbally or in writing.
   - You have one month to respond to a request.
   - The right is not absolute and only applies in certain circumstances. Contact the SAR Team should you receive a request of this nature.

e) The right to restrict processing - Individuals have the right to request the restriction or suppression of their personal data.
   - This is not an absolute right and only applies in certain circumstances.
   - When processing is restricted, the Council is permitted to store the personal data, but not use it.
   - An individual can make a request for restriction verbally or in writing.
   - The Council have one calendar month to respond to a request.
   - This right has close links to the right to rectification and the right to object. Contact the Data Protection Officer should you receive a request of this nature.

f) The right to data portability - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data Contact the Data Protection Officer should you receive a request of this nature.

g) The right to object Individuals have the right to object to:

   - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
   - direct marketing (including profiling); and
   - processing for purposes of scientific/historical research and statistics.

Objections where the Council processes personal data for the performance of a legal task or my organisation's legitimate interests?

Individuals must have an objection on "grounds relating to his or her particular situation". The Council must stop processing the personal data unless:

- it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
- or the processing is for the establishment, exercise or defence of legal claims.

The Council will inform individuals of their right to object "at the point of first communication" and in its Fair Processing Notice.

Objections where the Council processes personal data for direct marketing purposes?

The Council must stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse.

The Council must deal with an objection to processing for direct marketing at any time and free of charge.

The Council will inform individuals of their right to object "at the point of first communication" and in its Fair Processing Notice.

Objections where the Council processes personal data for research purposes?

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes. If the Council is conducting research where the processing of personal data is necessary for the performance of a public interest task, it is not required to comply with an objection to the processing.

Email: Data.Protection@cheltenham.gov.uk should you receive any requests outlining an objection to processing.

h) Rights in relation to automated decision making and profiling.

The UK GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement);
- and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The UK GDPR applies to all automated individual decision-making and profiling. This type of decision-making can only be done where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

If the Council is conducting this type of decision making it must:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

5.2. If you wish to process information in this way, then contact the Data Protection Officer prior to doing so.

6. Special Category Data

6.1. There are additional requirements placed upon the data controller where the holding of "special category data" is concerned. Special category data relates to the following:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

6.2. Where the Council processes any of the above categories of special personal data there should be higher levels of security in place and greater restrictions on sharing and processing this data. There will also be a need to complete a Data Protection Impact Assessment prior to commencing the processing.

7. Information Sharing

7.1. Where the Council regularly shares personal information with our partners and other organisations an Information Sharing Agreement should be put in place. This agreement is signed by all partners to the sharing and agrees a set of standards and best practice surrounding Data Protection.

7.2. Any Council department which shares personal information externally on a regular basis should email: Data.Protection@cheltenham.gov.uk for advice.

7.3. The Council is signed up to an Information Sharing Protocol, along with various other organisations in Gloucestershire. The protocol outlines the best practices surrounding the sharing of personal information and the agreed processes between partners whilst ensuring Data Protection law is adhered to.

7.4. Details of the Information Sharing Protocol can be found on the County Council's website.

8. Use of Personal Data in Marketing and Promotion

8.1. The Council complies with the Privacy of Electronic Communications Regulations (PECR).

8.2. PECR is a law in the UK which makes it unlawful to send direct marketing (or any promotional material with regards to goods and services) by electronic means without the consent of the receiver.

8.3. Further advice can be found on the intranet.

9. Responsibility of Staff and Members

9.1. All staff and elected members, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to personal data that they may handle in the course of their work.

9.2. All have a responsibility for Data Protection and are required to follow this policy.

9.3. All have a responsibility to ensure they have completed the mandatory Data Protection training, along with all other mandatory training under the Information Governance umbrella.

9.4. The Data Protection Policy sits in accordance with other policies in order to support UK GDPR compliance, these should be read in conjunction with the data Protection Policy.

9.5. The following policies contain further guidance in some areas of Data Protection – they are all available on the intranet:

- Information Governance Policy
- Data Retention Policy
- Anonymisation and Pseudonymisation Policy
- Privacy Notice Guidance
- Access to Information Rules – Part 4E of the Constitution
- Data Protection and Security Incident Reporting Policy

- Information Security and Acceptable Use Policy

10. Data Protection Governance

10.1. Information on the following will be reported quarterly to the Governance Group

- Training stats
- SAR requests
- Incidents (number and trends)

10.2. The reporting will be based around the following Key Performance Indicators (KPI's):

- 90% of incidents reported investigated in time frame as defined in the incident process
- 90% of incidents reported within timescales defined in incident process
- 90% of actions identified from incidents completed within timeframe
- 95% of staff completed the mandatory training
- 80% of SARs answered within statutory timeframes