Herefordshire Council

Data Protection Policy

Document information
Reference number

Approved by	Information Governance Steering Group
Date approved	2025
Version	2.0
Last revised	April 2025
Review date	May 2028
Category	Corporate Governance
Owner	Information Governance Manager
Target audience	All staff

After the Review Date has expired, this document may not be up to date. Please contact the document owner to check the status after the Review Date shown above.

This procedure may be reviewed earlier than the Review Date in the event of significant developments requiring changes to the document.

If you would like help to understand this document, or would like it in another format or language, please contact the document owner.

1.Introduction

Herefordshire Council has a responsibility under the Data Protection legislation to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. The council is committed to ensuring that it handles personal information in accordance with its obligations under the Data Protection legislation and professional guidelines.

The Data Protection legislation applies to all council employees, members, volunteers, contractors and staff members of any other bodies with whom we work who handle council data in joint teams.

This Policy is a statement of what the council does to ensure its compliance with the legislation. The council will use all appropriate and necessary means at its disposal to comply with the Data Protection legislation and associated guidance. This Policy provides a framework within which the council will ensure compliance with the requirements of the legislation and will underpin any operational procedures and activities connected with the implementation of the legislation.

2. Background

The Data Protection legislation governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals about whom data is held (the “data subjects”) can have a certain amount of control over the way in which that data is handled.

Some of the main requirements are:

- All data must be handled in accordance with the six Data Protection Principles (see Appendix 1)

- The data subject has various rights under the legislation:
  - To be informed about what personal data is being processed
  - To request access to that information
  - To request inaccuracies or incomplete data are rectified
  - To have personal data erased
  - To prevent or restrict processing in specific circumstances
  - To object to processing in specific circumstances
  - To object to automated decision making (including profiling) in specific circumstances
  - To object to data portability in specific circumstances

- Processing of data, including special categories of data, must be done under a lawful basis, meeting the conditions set out in Appendix 2. Special category data is information about race, ethnic origin, political persuasion, religious belief, trade union membership, genetics, biometrics (where used for identification purposes), health, sex life and sexual orientation.

- The Data Protection legislation deals with criminal offence data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.

- There is a principle of accountability of data controllers to implement:

- Appropriate technical and organisational measures that include internal data protection policies
- Staff training and awareness of the requirements of the Data Protection legislation
- Internal audits of processing activities
- Maintaining relevant documentation on processing activities
- Appointing a data protection officer
- Implementing measures that meet the principles of data protection by design and data protection by default, including data minimisation, pseudonymisation, transparency, and creating and improving security features on an ongoing basis.

- Data protection impact assessments (DPIA's) are carried out where appropriate as part of the design and planning of projects, systems and programmes.

- Data controllers must have written contracts in place with all data processors and ensure that processors are only appointed if they can provide 'sufficient guarantees' that the requirements of the legislation will be met.

- Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office (ICO) within 72 hours of the council becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the council will notify those individuals concerned directly.

- The ICO is responsible for regulation and issue notices and fines to organisations where they are not complying with the requirements of the Data Protection legislation. They also have the ability to prosecute those who commit criminal offences under the legislation.

3. Roles and Responsibilities

3.1 Data Protection Officer

The Data Protection Officer is responsible for the following tasks:

- Informing and advising the Council, any processor engaged by the council as data controller, and any employee of the council who carries out processing of personal data, of their obligations under the legislation.

- Providing advice on and monitoring of DPIA's.

- Co-operating with the ICO.

- Ensure council policies adhere to legislative requirements regarding personal data.

- Monitoring compliance by the council with the legislation.

- Raising awareness of data protection requirements and ensuring that staff are trained.

- Conducting data protection audits

The council must provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined above and to maintain their expert knowledge of data protection law and practice.

3.2 Information Governance Manager

Is responsible for the oversight of the Information Governance functions, including the work of the Information Governance team and the Data Protection Officer.

The Manager (or their representative) will also report bi-annually to directors on activities and incidents to ensure the organisation complies with its responsibilities under the legislation.

3.3 Corporate Leadership Team

The Corporate Leadership Team will be responsible for ensuring that the organisation complies with its responsibilities under the Data Protection legislation through monitoring of activities and incidents via at least bi-annual reporting by the Information Governance Manager (or their representative). The Corporate Leadership Team will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the Data Protection legislation, and in particular that there is capacity within Information Governance to support compliance.

3.4 Information Governance Steering Group

The Group will be responsible for discussing and resolving any data protection and confidentiality issues which may arise, approve information governance policies and protocols, monitor activities and incidents via monthly reporting by the Information Governance team and escalate issues where appropriate to the Corporate Leadership Team.

3.5 Corporate Directors / Service Directors / Heads of Service / Service Managers / Team Leaders

All Corporate Directors, Service Directors, Heads of Service, Service Managers and Team Leaders will be fully aware of their responsibility with regards to the Data Protection legislation.

They will ensure that:

- All staff for which they are responsible are provided with and undertake appropriate training with regards to the requirements of the legislation and their responsibilities under it.
- Information is created and stored in accordance with the council's Records Management policies and procedures.
- Information is handled in a secure and confidential manner.
- They inform the Information Governance team of all data breaches in their area as soon as they become aware of the breach.

- Information is supplied in relation to subject access requests in a timely manner.
- Privacy notices are in place for the processing of personal data within their area.
- DPIA's are carried out as appropriate.
- They comply with Data Protection Audits as and when required.

3.6 Information Governance Team

The Information Governance Team will:

- Produce and maintain up-to-date policies and procedures to ensure compliance with current legislation and guidelines.
- Produce training packages to ensure staff are fully aware of their responsibilities under the legislation.
- Audit processes and procedures to ensure staff both understand and comply with their responsibilities under the legislation.
- Support members of staff to conduct appropriate DPIA's and reviews.
- Work with the Data Protection Officer and Information Governance Manager to ensure organisational wide compliance with Data Protection legislation.

3.7 Social Care

Children's and Adults social care services will ensure that there is resource available to process subject access requests for files, supported by the Information Governance team.

3.8 All staff

It is the responsibility of all staff to ensure that they comply with the requirements of this policy and any associated policies or procedures. Failure to do so may result in disciplinary action being taken.

All staff will ensure that:

- Personal information is treated in a confidential manner in accordance with this and any associated policies.
- The rights of the data subjects are respected at all times.
- Personal information is only used for the stated purpose, as detailed in the relevant privacy notice.
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.

- Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.
- Personal information is recorded accurately and is kept up to date.
- They adhere to the council's Records Management Policy and associated policies and procedures to facilitate easy location of records as required.
- They refer any potential or actual Subject Access Requests (SAR's) to the Information Governance team upon receipt.
- They raise actual or potential breaches of the Data Protection legislation to the Information Governance team as soon as the breach is discovered.
- DPIA's are carried out as appropriate.

3.9 Contractors and Employment Agencies

Where a contractor or employment agencies are used, the contracts between the council and these third parties should contain mandatory information assurance clauses to ensure that the contract staff are bound by the same code of behaviour as council members of staff in relation to the Data Protection legislation.

3.10 Volunteers

All volunteers are bound by the same code of behaviour as council members of staff in relation to the Data Protection legislation.

3.11 Members

Where members are working in their capacity as councillors for Herefordshire Council they are bound by the same code of conduct as council members of staff in relation to Data Protection legislation.

4. Records Management

Good records management practice plays a pivotal role in ensuring that the council is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meet the requirements of the legislation. It is necessary to ensure that robust records management practices are in place which are understood and implemented by all staff dealing with records within the council.

It is the responsibility of all staff to ensure that they are familiar with the policies, procedures and schedules relating to records management within the council, these include:

- Records Management Policy

- Retention Schedules
- Version Control Procedure
- File Naming Procedure

All records should be retained and disposed of in accordance with the council's retention schedules.

5. Legal Processing Conditions

Much of the council's processing of personal data will be done under a legal obligation or public task.

Members of staff, volunteers and contractors should ensure they use the correct processing condition (see Appendix 2) before using information.

The council will take all reasonable steps to ensure that service users, members of staff, volunteers, and contractors are informed of the reasons the council requires information from them, how that information will be used and who it will be shared with. This will enable the data subject to give explicit informed consent to the council handling their data where the legal basis for processing is consent.

Should the council wish to use personal data for any purpose other than that specified when it was originally obtained, the data subject's explicit consent should be obtained prior to using the data in the new way unless such use is in accordance with other provisions of the legislation.

Should the council wish to share personal data with anyone other than those recipients specified at the time the data was originally obtained, the data subject's explicit consent should be obtained prior to sharing the data, failure to do so could result in a breach of confidentiality.

6. Accuracy and Data Quality

The council will ensure that all reasonable steps are taken to confirm the validity if personal information directly with the data subject.

All members of staff must ensure that service user personal information is checked and kept accurate and up to date on a regular basis, for example, by checking it with the service user when they attend for appointments in order that the information held can be validated.

Where a member of the public exercises their right for their data to be erased, rectified, or restricted or where a member of the public objects to the processing of their data, the Information Governance team must be notified and the appropriate procedures followed.

7. Subject Access Requests

All staff must ensure that requests for the personal information of living individuals made under the Data Protection legislation is dealt with in accordance with the council's procedure for processing subject access requests.

8. Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications Regulations 2003 as amended set out the requirements for respecting privacy with electronic communications. The regulations include the use of cookies on websites and actions that can be defined as marketing activities within the Regulations.

9. Data Protection Impact Assessments (DPIA's)

A DPIA is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information. They must be carried out at the early stages of projects and are embedded into the council's decision-making process. Support and advice on completing these can be obtained from the Information Governance team.

10. Data Processors

A data processor is a third-party individual or organisation carrying out a data processing activity on behalf of the council.

The council must have written contracts in place with all data processors. The council will ensure that processors are only appointed if they can provide 'sufficient guarantees' through the procurement process that the requirements of the legislation will be met and the rights of data subjects protected.

11. Complaints

A formal complaint from an individual with reference to the council's handling of personal information will be handled under the council's complaints processes as outlined in the Corporate Complaints Policy

Complaints or expressions of dissatisfaction with responses to Subject Access Requests will be handled under the Internal Review Procedure for Subject Access Requests.

Should the complainant remain dissatisfied with the outcome of their complaint to the council once the complaints procedure has been exhausted, a complaint can be made to the ICO who will then investigate the complaint and take action where necessary.

12. Security and Confidentiality

All staff must ensure that information relating to identifiable individuals is kept secure and confidential at all times. The council will ensure that its holdings of personal data are properly secured from loss or corruption and that no unauthorised disclosures of personal data are made. Further information can be found in the information security policies and procedures.

The council will ensure that information is not transferred to countries outside the European Economic Area (EEA) unless that country has an adequate level of protection for security and confidentiality of information.

13. Risks

The risks in inadequate data protection compliance (including when using data processors) are:

- Complaints from the community if their privacy rights are violated
- Notices from the ICO
- Loss of reputation through a lack of trust by the community in handling confidential information
- Incurring of monetary penalties if a breach of the Data Protection legislation occurs

14. Monitoring and Audit

The Information Governance Manager (or their representative) will be responsible for compiling a bi-annual report for directors, which provides details of compliance with the Data Protection legislation. A monthly report will be produced by the Information Governance team summarising compliance through areas including subject access and security incident reporting.

This policy and associated procedures will be monitored by the Information Governance Steering Group. Compliance will also be monitored through internal audit.

15. Review

This policy will be reviewed as it is deemed appropriate, but at least every 3 years.

Author: Claire Jacobs, Information Governance Manager
Status: Final
Responsible Corporate Director: Claire Porter, Director Governance & Law
Approval: Information Governance Steering Group (final draft) / SIRO (final)
Date Approved: 1 May 2025
Publisher: Herefordshire Council

Security classification: Open
Publication: Internal & External
Category: Corporate; information governance
Date for review: April 2028

Reference number:

Appendix 1 – Data Protection Principles

First Principle

Processed lawfully, fairly and in a transparent manner in relation to individuals;

Second Principle

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 to be incompatible with the initial purposes;

Third Principle

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Fourth Principle

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;

Fifth Principle

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 subject to implementation of the appropriate technical and organisational measures required by the UK General Data Protection Regulations (GDPR) in order to safeguard the rights and freedoms of individuals;

Sixth Principle

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.

Appendix 2: Processing Conditions

Article 6 Conditions: Lawful basis for processing data:

(a) Consent

The individual has given clear consent for you to process their personal data for a specific purpose

(b) Contract

The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

(c) Legal obligation

The processing is necessary for you to comply with the law (not including contractual obligations)

(d) Vital interests

The processing is necessary to protect someone's life

(e) Public task

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

Article 9: Lawful basis for processing special category data

Processing of special category data is permitted:

a) Explicit consent

If the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

b) Employment, social security and social protection law

If the processing is necessary for the purposes of carrying out the obligations and exercising specific right of the controller or data subject in the field of employment and social security and social protection law; in so far as it is authorised by Domestic Law; providing for appropriate safeguards for the fundamental rights and interests of the data subject.

c) Vital interests

If processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

d) Not-for-profit bodies

If processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit bodies with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

e) Made public by the data subject

Processing relates to personal data which are manifestly made public by the data subject.

f) Legal claims and judicial action

Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) Substantial public interest

Processing is necessary for reasons of substantial public interest, on the basis of Domestic Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h) Health and Social Care

Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment of the management of health or social care systems and services on the basis of Domestic Law for pursuant to contracts with a health professional and subject to the conditions and safeguards.

i) Public Health

Processing is necessary for reasons of public health in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Domestic Law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

j) Archiving, research and statistics

Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Domestic Law which shall be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.