Herefordshire Council

Reference number	
Approved by	**Information Steering Group**
Date approved	**February 2018**
Version	**1.0**
Last revised	**January 2018**
Review date	**January 2021**
Category	**Information Assurance**
Owner	**Data Protection Officer**
Target audience	**All staff**

DATA PROTECTION POLICY

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.

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

CONTENTS

1. Introduction

Herefordshire Council has a responsibility under the Data Protection Act 2018 to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. This Policy is a statement of what the Council does to ensure its compliance with the Act.

The Data Protection Policy applies to all Council employees, members, volunteers, contractors and to staff members of any other bodies with whom we work who handle council data in joint teams. The Policy provides a framework within which the Council will ensure compliance with the requirements of the Act and will underpin any operational procedures and activities connected with the implementation of the Act.

2. Background

The Data Protection Act 2018 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 it is handled.

Some of the main features of the Act are:

- All data covered by the Act must be handled in accordance with the Six Data Protection Principles (see Appendix 1)

- The person about whom the information is held (the Data Subject) has various rights under the Act including the right to be informed about what personal data is being processed, the right to request access to that information, the right to request that inaccuracies or incomplete data are rectified, and the right to have personal data erased and to prevent or restrict processing in specific circumstances. Individuals also have the right to object to processing based on the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling); and processing for the purposes of scientific/historical research and statistics. There are also rights concerning automated decision making (including profiling) and data portability.

- Processing of data, including special categories of data, must be done under a lawful basis, meeting the conditions set out in Appendix 2. This data includes 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 Act 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 Act, internal audits of processing activities, maintaining relevant documentation on processing activities, appointing a data protection officer, and 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 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 Act will be met and the rights of data subjects protected.

- 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 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 Information Commissioner is responsible for regulation and issue notices to organisations where they are not complying with the requirements of the Act. She also has the ability to prosecute those who commit offences under the Act and to issue fines.

3 Policy Statement

The Council is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under the Data Protection Act 2018 and professional guidelines. The Council will use all appropriate and necessary means at its disposal to comply with the Data Protection Act and associated guidance.

4 Roles and Responsibilities

4.1 Data Protection Officer

The Data Protection Officer is the Corporate Customer Information and Equality Manager, and they are 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 that person's obligations under the legislation
- providing advice and monitoring for the carrying out of a data protection impact assessments
- co-operating with the Information Commissioner's Office,
- acting as the contact point for the Information Commissioner's Office
- monitoring compliance with policies of the council in relation to the protection of personal data
- monitoring compliance by the council with the legislation.

In relation to the policies mentioned above, the data protection officer's tasks include—

(a) assigning responsibilities under those policies,

(b) raising awareness of those policies,

(c) training staff involved in processing operations, and

(d) conducting audits required under those policies.

The Data Protection Officer is also responsible for the oversight of the Information Governance and the Information Access functions.

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.

4.2 Management Board

The Management Board will be responsible for ensuring that the organisation complies with its responsibilities under the Data Protection Act through monitoring of activities and incidents via at least bi-annual reporting by the Data Protection Officer. The Board will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the Data Protection Act, and in particular that there is capacity within Information Governance to support compliance.

4.3 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 and information access policies and protocols, monitor activities and incidents via monthly reporting by the Data Protection Officer, and escalate issues where appropriate to Management Board.

4.4 Directors/Assistant Directors/Heads of Service/Service Managers/Team Leaders

All Directors, Assistant Directors, Service Managers and Team Leaders will be fully aware of their responsibility with regard to the Data Protection Act. This will be accomplished through inclusion in staff contracts and job descriptions, coupled with the provision of appropriate awareness training, supported by local policies and procedures detailing organisational and individual responsibilities and action required to ensure compliance with the Act.

They will ensure that:

- All staff for which they are responsible are provided with appropriate training with regard to the requirements of the Act and their responsibilities under it.
- Information is created and stored in accordance with the Council's Records Management Policy and Procedures to facilitate easy location should it be required and to ensure that records are retained in line in particular with the Third, Fourth and Fifth Principles of the Act.
- Information is handled in a secure and confidential manner.
- The Data Protection Officer via the Information Governance Team is informed 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.
- Data protection impact assessments are carried out as appropriate.
- They comply with Data Protection Audits as and when required.

4.5 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 Act;

- Audit processes and procedures to ensure staff both understand and comply with their responsibilities under the Act.

- Support members of staff to conduct appropriate data protection impact assessments and reviews.

- Work with the Data Protection Officer to ensure organisation wide compliance with the Act

- Work with council departments, and where appropriate with partner organisations, to ensure that appropriate mechanisms are in place to raise staff awareness within the Council.

4.6 Legal Services

Legal Services will:-

- Provide advice and assistance on matters relating to the Data Protection Act as required.

.4.7 Social Care

Social Care services for children and for adults will ensure that there is resource available to process subject access requests for files, supported by the Information Governance and the Information Access Team.

4.8 All Staff

All Staff will ensure that:-

- Personal information is treated in a confidential manner in accordance with this and any associated policies.

- The rights of data subjects are respected at all times.

- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.

- 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 create and maintain their own records in accordance with the Council 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 to the Information Governance Team.

- They raise actual or potential breaches of the Data Protection Act to the Data Protection Officer via the Information Governance Team as soon as the breach is discovered.

- Consent is obtained before using cookies on web sites.

- Data protection impact assessments are carried out as appropriate.

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.

4.9 Contractors and Employment Agencies

Where contractors 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 Act.

4.10 Volunteers

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

4.11 Members

Where members are working in their capacity as councillors for Herefordshire Council, are bound by the members code of behaviour in relation to the Data Protection Act.

5 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 Act. 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.

6 Consent

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 Act.

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

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

7 Accuracy and Data Quality

The council will ensure that all reasonable steps are taken to confirm the validity of 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 Data Protection Officer must be notified via the Information Governance Team and the appropriate procedures followed.

8 Subject Access Requests

All staff must ensure that requests for the personal information of living individuals made under the Data Protection Act 2018 are dealt with in accordance with the council's procedures for processing subject access requests.

9 Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications Regulations 2003 set out requirements for respecting privacy with electronic communications. The Regulations have been amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. The rules include websites wanting to use cookies to get consent, and they also affect the council if the council carries out actions that can be defined as marketing within the Regulations.

10 Data Protection Impact Assessments

A data protection impact assessment 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 in to the council's decision making process.

11 Providers

The council must have written contracts in place with all suppliers who process personal data on behalf of the council as "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 Act will be met and the rights of data subjects protected.

The council's key providers include:

- Balfour Beatty
- FCC
- Hoople

12 Complaints

Any expression of dissatisfaction from an applicant with reference to the council's handling of personal information will be treated as a complaint, and handled under the council's complaint's processes as outlined in the access to information policy.

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 Information Commissioner who will then investigate the complaint and take action where necessary.

13 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 and this has been confirmed by the Information Commissioner.

14 Informing Staff of Data Protection Requirements

The council will inform staff of their responsibilities under the Data Protection Act through the normal communication mechanisms within the council, coupled with induction and refresher training and the cascade of information via Heads of Service/Service Managers/Team Leaders in line with their responsibilities detailed at Section 4.4.

15 Reporting

The Data Protection Officer will be responsible for compiling an annual report for the Management Board, which provides details of compliance with the Data Protection Act. A monthly report will be produced by the Information Governance Team summarising compliance through areas including subject access and security incident reporting.

16 Monitoring and Audit

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

17 Associated Legislation and Guidance

- Access to Health Records Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Crime and Disorder Act 1988
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Privacy and Electronic Communications Regulations 2003
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

18 Risks

The risks of not ensuring adequate data protection compliance (including when using provider services as data processors on behalf of the Council as data controller) are:

- incurring of monetary penalties if a breach of the Data Protection Act occurs
- complaints from the community if their privacy rights are violated
- loss of reputation through a lack of trust by the community in handling confidential information

The Information Governance risk register will include any specific data protection risks and actions taken to mitigate them.

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 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

CONDITIONS FOR PROCESSING PERSONAL DATA

The lawful bases for the council to process personal data are set out below. At least one of these must apply whenever the council processes personal data:

(a) Consent: the individual has given clear consent for the council to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract the council has with the individual, or because they have asked the council to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for the council 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 the council to perform a task in the public interest or for the council's official functions, and the task or function has a clear basis in law.