Data Protection Policy

Author: Rachel Everitt

Date: September 2024

Version: v0.1

Title	**Data Protection Policy**
Author	**Rachel Everitt**
Owner	**Data Protection Officer**
Created	**September 2024**
Approved by	**Audit Committee**
Date of Approval	**February 2025**
Review Date	**February 2027**

Document Version Control

Document Version Control	
Issue Number	Date
0.01	September 2024

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

The processing of personal data is essential to many of the services and functions carried out by Bury Council. This data includes that about members of the public, current, past and prospective employees, service users, clients, customers and suppliers. The Council recognises that compliance with data protection legislation (including the Data Protection Act, the UK General Data Protection Regulation and other related legislation) ensures that the processing of this data is carried out fairly, lawfully and transparently.

The council has policies and procedures in place to ensure all employees, elected members, contractors, consultants and partners who have access to any personal data held on or behalf of the council, are fully aware of, and abide by their duties and responsibilities under this legislation.

This policy is part of Bury Council's Information Governance Framework and should be read in conjunction with the other policies and procedures within the framework.

Scope

This policy applies to the collection, use, sharing and other processing of all personal data held by Bury Council in any format including, paper, electronic, audio and visual. It applies to all permanent and temporary staff employed by the council.

Data protection principles

The UK General Data Protection Regulations (GDPR) sets out seven key principles which lie at the heart of data protection and which the council must comply with:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) 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 ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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 ('accuracy');

(e) 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 ('storage limitation');

(f) 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 ('integrity and confidentiality').

2. Policy

Personal and Special Category data

Personal data is defined as data relating to a living individual (a data subject) who can be identified, directly or indirectly, from that data.

Special Category personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs

- Trade union membership
- Physical or mental health or condition
- Sexual life
- Biometrics (where used for identification)

There are separate safeguards for personal data relating to criminal convictions and offences – see Article 10 of the UK GDPR.

Lawful basis for processing personal data

Processing personal data is only legal if there is a lawful basis to do so. The lawful bases for processing are set out in Article 6 of the UK GDPR.

The council will ensure that at least one of these will apply whenever personal data is processed:

(a) **Consent:** the individual has given clear consent for their personal data to be processed for a specific purpose.

(b) **Contract:** the processing is necessary for a contract with the individual.

(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 official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform official tasks.)

Conditions for processing special category data

Processing special category data is prohibited unless a lawful exemption applies.

The conditions for processing this data are set out in Article 9 of the UK GDPR.

The council will ensure that at least one of these will apply whenever special category data is processed:

(a) The individual has given clear consent for their personal data to be processed for a specific purpose.

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

(c) 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) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body 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) Processing relates to personal data which are manifestly made public by the data subject

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

(g) Processing is necessary for reasons of substantial public interest

(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

(i) Processing is necessary for reasons of public interest 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

Law Enforcement Purposes

The UK GDPR does not apply to sensitive processing for law enforcement purposes, which is covered by Part 3 of the Data Protection Act 2018 where sensitive processing is defined as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

Law enforcement purposes are defined as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Sensitive processing for law enforcement purposes is only permitted when:

- the data subject has given consent to the processing for the specific purpose or
- the processing is strictly necessary for a law enforcement purpose, the processing meets at least one condition in Schedule 8 of the Act

Bury Council is classed as a Competent Authority for Law Enforcement purposes and is permitted to carry out sensitive processing as defined in Schedule 8 of the Act. Those conditions are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest.
- necessary for the administration of justice.
- necessary to protect the vital interests of the data subject or another

individual.

- necessary for the safeguarding of children and of individuals at risk.
- personal data already in the public domain (manifestly made public).
- necessary for legal claims.
- necessary for when a court acts in its judicial capacity.
- necessary for the purpose of preventing fraud.
- necessary for archiving, research or statistical purposes.

The Council services that undertake law enforcement sensitive processing will only do so when it is necessary to fulfil our function as a public body, or with the consent of the individual, and where it has a lawful basis to do so, and the information is required for a specific reason.

Handling of Personal/Special Category Data

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

- Fully observe conditions regarding the fair collection and use of personal information.
- Specify the purposes for which information is used.
- Collect and process information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Determine the length of time information is held.
- 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. These include:
    - The right to be informed
    - The right of access to one's personal information
    - The right to rectification

- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

If an individual makes a request relating to any of the rights listed above, the council will consider each request in accordance with all applicable data protection laws and regulations. The council has separate policies outlining how we manage and deal with:

- Freedom of Information Requests
- Environmental Information Regulations
- Subject Access Requests

No administration fee will be charged for complying with such a request unless the request is deemed to be unnecessary, excessive in nature, or a repeated request.

In addition, Bury Council will ensure that:

- There is specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone handling personal information is appropriately trained to do so and is appropriately supervised.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance of handling data subject requests is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All managers and staff within the council will take steps to ensure that personal data is kept secure at all times both on council premises and any other venue employees may be working from, including those working from home, to prevent unauthorised or unlawful, loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected by appropriate technical and organisational measures.

All staff and managers who work from home, will ensure that they are aware of and abiding by the Individual Home Working Policy.

When engaging the services of contractors, consultants, partners or other agents, the Council will ensure:

- that they and their staff who have access to personal data held or processed for or on behalf of the council, are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the council and that individual, company, partner or firm.
- that any contracts/arrangements allow for data protection audits by the council of data held on its behalf (if requested).

Councillors/Members of Parliament (MP)

The council will share personal data with councillors/MPs in the following circumstances:

- the councillor/MP represents the ward in which the data subject lives.
- the councillor/MP makes it clear that they are representing the data subject.
- the information requested is necessary to respond to a data subject's query/complaint. Consent from the data subject is **not** required in these circumstances.

Data Protection Responsibilities

In compliance with the UK GDPR, the council has an appointed Data Protection Officer (DPO).

The DPO has overall responsibility for monitoring internal compliance, informing and advising on data protection obligations, and acts as a contact point for data subjects.

The DPO is responsible for ensuring:

- this Policy is implemented.
- the provision of data protection training for staff within the council.
- for the development of best practice guidelines.
- for carrying out compliance checks to ensure adherence with data protection legislation throughout the authority.

Notification of Data Breaches

The council employs a robust information security incident management process. All staff are obliged to report any incidents involving information to ensure they are dealt with.

A data breach is a type of information security incident where the confidentiality, integrity or availability of personal data has been affected. The council will review incidents to assess if the risk to the rights and freedoms of the data subject(s) is likely to occur. In accordance with the UK GDPR, where the risk is likely, the council will report the data breach to the ICO within 72 hours.

Information Commissioner Registration

The ICO maintains a public register of data controllers and data protection officers. Bury Council's registration number is XXXXX.

The Data Protection Act 2018 requires every data controller, who is processing personal data, to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

3. Compliance and Monitoring

Legal and Professional Obligations

Bury Council will take actions to comply with the relevant legal and professional obligations.

Training

Bury Council will provide relevant training both online and face to face to ensure that staff understand the legislation and its application to their role.

All staff must complete mandatory data protection training every year and undertake any further training provided by Bury Council to enable them to perform their duties appropriately specifically those staff responding to complaints, Subject Access Requests and Freedom of Information requests.

Completion of training will be monitored by the Policy and Compliance Team and all employees must have regard to the Data Protection Legislation and this policy when collecting, accessing, using, disclosing or destroying personal information. Failure to do so may result in disciplinary action and legal prosecution.

If an employee is in any doubt about how to handle personal or special category data they should speak to their line manager or contact the Policy and Compliance Team by emailing IG@bury.gov.uk.

Policy Review

This policy will be reviewed regularly by the Policy and Compliance Team to ensure that it is updated in line with any change in legislation.

Bury Council will continue to review the effectiveness of this policy to ensure that it is achieving it intended purpose.

Any breaches of the principles in this policy must be reported to the Policy and Compliance Team immediately; ig@bury.gov.uk.

Where staff fail to follow and comply with this policy it may result in disciplinary action via the HR channels.

4. Policy exemption

Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs.

Where the significance and purpose of the data does not justify a particular aspect (for example the cost of building an internal system validation check outweighs the benefit of the additional data accuracy) then this should be risk assessed on a case-by-case basis. Where there are justifiable reasons, the Data Protection Officer must be consulted immediately using ig@bury.gov.uk.