

Data protection policy

Protecting personal information and respecting individual rights

Author: Information Governance

Contact: dataprotection@luton.gov.uk

Version: 1.7

Last updated: August 2026

Contents

1 Introduction	2
2 Scope.....	2
3 Data protection principles.....	2
5 Lawful basis for processing data.....	2
6 Data protection roles.....	3
7 Personal data in the public domain	3
8 Responsibilities of staff and contractors.....	3
9 Data security	3
10 Sending personal data securely.....	3
Email	3
11 Data breaches.....	4
12 Data subject rights	4
13 Prohibited activities	4
14 Data protection by design and default.....	4
16 International transfers	5
17 Privacy and electronic communications regulations.....	5
18 Exemptions	5
19 Conclusion	5
20 Definitions	5

1 Introduction

We recommitted to protecting the rights and freedoms of individuals when processing personal data. This policy must be followed by all staff, contractors and partners working on our behalf.

2 Scope

We must comply with the Data Protection Act 2018, the UK General Data Protection Regulation, the Privacy and Electronic Communications Regulations and the Data (Use and Access) Act 2025. This policy applies to personal data held electronically or on paper and processed for council purposes.

The same standards apply to workforce, resident and service-user information. Processing includes collecting, recording, storing, using, sharing, amending, erasing and destroying data.

3 Data protection principles

Personal data must be processed lawfully, fairly and transparently; collected for specified and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date; retained only as long as necessary; and protected using appropriate technical and organisational measures. We must also be able to demonstrate compliance.

4 Caldicott guardian principles

- Justify each purpose for using confidential information.
- Do not use personal confidential data unless it is necessary.
- Use the minimum information required.
- Restrict access to people with a genuine need to know.
- Ensure everyone understands their responsibilities.
- Comply with the law.
- Recognise that the duty to share information can be as important as the duty to protect confidentiality.

5 Lawful basis for processing data

5.1 Personal data

A lawful basis must be identified before processing personal data: consent, contract, legal obligation, vital interests, public task or legitimate interests. As a public authority, we may rely on legitimate interests only for genuine and necessary organisational activity outside its official public tasks.

5.2 Special category data

Processing special category data requires both an Article 6 lawful basis and an Article 9 condition. Conditions include;

- explicit consent
- employment and social protection
- vital interests
- not-for-profit bodies
- information made public by the individual
- legal claims
- substantial public interest

- health or social care
- public health
- research
- statistics or archiving

Seek advice from dataprotection@luton.gov.uk where a condition in the Data Protection Act 2018 is required.

6 Data protection roles

Senior information risk owner

Leads our information-risk culture, owns the information-risk framework and advises the Chief Executive.

Caldicott guardian

Safeguards confidentiality, reviews protocols and acts as our conscience for health and social care information.

Data protection officer

Monitors compliance, provides advice and training, supports DPIAs and information-sharing arrangements, and acts as the contact point for the Information Commissioner's Office.

7 Personal data in the public domain

Some information is published as part of our statutory functions, such as planning applications. The names and work contact details of employees at service-manager level and above may also be made public where appropriate.

8 Responsibilities of staff and contractors

- Complete mandatory data-protection training on joining and annual refresher training.
- Process personal data only in line with data-protection law and this policy.
- Follow council guidance and seek advice where needed.
- Contact Information Governance at dataprotection@luton.gov.uk or extension 7700.

9 Data security

- Keep passwords secure and never share them.
- Secure paper records and do not leave them unattended.
- Protect hard-copy documents taken out of the office.
- Use encrypted, password-protected council devices and approved storage.
- Lock removable media, laptops and other devices away when not in use.

10 Sending personal data securely

Email

Use our approved secure-transfer service for sensitive information and confirm receipt when appropriate.

Hard copy

Check the recipient's identity and address, use a sealed envelope and select tracked or special delivery where the sensitivity warrants it.

Encrypted device

Where necessary, use a council-approved encrypted device and provide the password through a separate channel.

11 Data breaches

Report suspected data breaches immediately to a line manager or suitable colleague. Complete our data-breach report as quickly as possible and no later than 24 hours after discovery. Information Governance will assess containment, risk and any requirement to notify the Information Commissioner's Office within 72 hours.

12 Data subject rights

- To be informed about processing.
- To access personal data.
- To rectify inaccurate or incomplete data.
- To request erasure where the right applies.
- To restrict processing.
- To data portability in applicable circumstances.
- To object to processing.
- To safeguards concerning solely automated decision-making and profiling.

Most requests must be answered within one calendar month. Rights may be restricted where legislation permits. Seek advice before refusing or limiting a request.

13 Prohibited activities

- Sharing or exposing passwords.
- Sending council data to personal email accounts.
- Sending information to unauthorised recipients or by insecure means.
- Losing, misplacing or leaving personal data unprotected.
- Accessing records without a legitimate business reason.
- Making unauthorised copies, photographs or screenshots.
- Using council-held personal data for private purposes.
- Disclosing data outside of the council without a lawful basis.

Breaches of this policy may be dealt with under our disciplinary procedures and may lead to dismissal, depending on seriousness.

14 Data protection by design and default

Data protection must be considered from the start and throughout the life of every system, project and process. Use the minimum identifiable data required, limit access, set privacy-protective defaults, retain data only as long as necessary and use pseudonymisation where appropriate.

15 Data protection impact assessments

A DPIA is required where processing is likely to result in high risk, including large-scale sensitive-data processing, systematic monitoring, significant automated decisions, innovative technologies, biometrics, data matching, invisible processing or processing involving vulnerable people.

Complete the pre-assessment and obtain Information Governance advice before processing begins.

16 International transfers

Personal data may be transferred outside the UK only where data-protection law permits it. An adequacy regulation, appropriate safeguard or specific legal exception must apply, and the decision must be documented. Seek Information Governance advice before arranging an international transfer.

17 Privacy and electronic communications regulations

Communications necessary for our official functions are not direct marketing. Where messages do constitute direct marketing, we must comply with PECR and data-protection requirements, including applicable consent and objection rights.

18 Exemptions

Exemptions are limited legal provisions. They must be necessary, proportionate, justified and documented. An exemption does not remove the need for a lawful basis. Seek Information Governance advice before relying on one.

19 Conclusion

Compliance is the responsibility of all staff, contractors and partners. Questions should be sent to dataprotection@luton.gov.uk.

20 Definitions

Personal data: Information relating to an identified or identifiable living person.

Special category data: Personal data requiring additional protection, including health, racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetic data, biometric identification data, sex life and sexual orientation.

Controller: The organisation that determines why and how personal data is processed.

Processor: An organisation or person processing personal data on behalf of a controller.

Data subject: The living individual to whom personal data relates.

Personal data breach: A security breach causing accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

DPIA: A structured assessment used to identify and reduce privacy risks before high-risk processing begins.