Data protection policy

Author: Business Intelligence

Contact: dataprotection@luton.gov.uk

Version: 1.6

Last updated: June 2024

Contents

1 Introduction 3
2 Scope 3
3 Data protection principles 3
4 Caldicott Guardian principles 4
5 Lawful basis for processing data 4
5.1 Personal data 4
5.2 Special category data 5
6 Data protection roles 6
7 Personal data in the public domain 6
8 Responsibilities of staff and contractors 6
9 Data security 7
10 Sending personal data securely 7
11 Data breaches 8
12 Data subject rights 8
13 Prohibited activities 10
14 Data protection by design and default 11
15 Data Protection Impact Assessments (DPIA) 12
16 International transfers 12
17 Exemptions 13
18 Conclusion 13
19 Definitions 13

1 Introduction

1.1 Luton Council is committed to protecting the rights and freedoms of all individuals in relation to the processing of their personal data. This policy should be followed by all staff, contractors and partners working on behalf of the council.

2 Scope

2.1 The Council needs to comply with the Data Protection Act 2018 and UK General Data Protection Regulations (UK GDPR). This policy has been developed to ensure all staff, contractors and partners understand their obligations when processing personal and special category data.

2.2 This policy and the legislation apply to all personal data, both that held in paper files and electronically. So long as the processing of the data is carried out for council purposes, it applies regardless of where data is held.

2.3 'Processing' data is widely defined and includes obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

3 Data protection principles

As outlined in Article 5(1) of the UK GDPR, personal and special category data must be:

Processed lawfully
All personal and special category data must be processed lawfully, fairly and in a transparent manner in relation to individuals.

Used for a specific purpose
The data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Be relevant to the purpose
The data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Be accurate
Data should be 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 no longer than necessary
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
- 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

Kept securely
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.

In addition to the above, article 5(2) adds that “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1. This is referred to as the seventh principle, **‘accountability’.**

4 Caldicott Guardian principles

In addition to the data protection principles, employees dealing with health and social care information must follow the Caldicott principles when processing Information relating to service users. The need for confidentiality also extends to other individuals, including relatives and staff as follows.

Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Don’t use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for data subjects to be identified should be considered at each stage of satisfying the purpose(s).

Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data are made fully aware of their responsibilities and obligations to respect confidentiality.

Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

The duty to share information can be as important as the duty to protect confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

5 Lawful basis for processing data

5.1 Personal data

You must have a lawful basis for collecting and processing personal data. These are as follows.

Consent
The data subject has given clear consent for us to process their personal data for a specific purpose.

Contract
The processing is necessary for a contract we have with the data subject, or because they have asked us to take specific steps before entering into a contract.

Legal obligation
The processing is necessary for us to comply with the law.

Vital interests
The processing is necessary to protect the data subject's life.

Public task
The processing is necessary for us to perform a task in the public interest or for our official functions as a public authority.

5.2 Special category data

In order to process special category data (see section 19 for definition) you must determine your lawful basis above and the special category condition below.

Explicit consent
The data subject has given clear consent for us to process their personal data for a specific purpose.

Employment, Social Security/Social Protection *
The data is necessary for employment or social security purposes.

Vital Interests
The processing is necessary to protect the data subject's life.

Not for profit
The data is processed by a not-for-profit body that the data subject belongs to i.e a trade union.

Public domain
The data subject has already made their information publicly available.

Legal defence claims
It is necessary for legal cases or by the courts.

Substantial public interest *
It is for the benefit of society as a whole.

Adult social care*
It is necessary to deliver health or social care services.

Public Interest in public health *
It is necessary to protect public health.

Scientific/historical Research, Statistics or Public Archiving *
It is necessary for archiving, research, or statistical purposes

*If authorised by law/with a basis in law – to rely on any of these, please seek advice from dataprotection@luton.gov.uk as an additional condition needs to be met:

("Employment, Social Security and Social Protection", "Adult Social Care", "Public Interest in public health", "Scientific/historical Research, Statistics or Public Archiving" – Schedule 1 of the DPA 2018.

"Substantial public interest" – Part 2 of Schedule 1 of DPA 2018)

6 Data protection roles

There are three core data protection roles in place to support the council's approach to data protection.

Senior Information Risk Owner

- Leads and fosters a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Owns the organisations overall information risk policy and risk assessment processes and ensuring they are implemented consistently
- Advises the Chief Executive on the information risk aspects on the Statement of Governance
- Owns the organisations information incident management framework

Caldicott Guardian

- Acts as a guardian, responsible for safeguarding the confidentiality of data subjects' information.
- Agrees and reviews internal protocols
- Develops security and confidentiality policies
- Acts as the 'Conscience of the Council - Provides a sense of right and wrong'

Data Protection Officer

- Monitors compliance with the GDPR and Data protection Act 2018
- Develops data protection policies, awareness-raising, training, and audits.
- Provides advice and on all aspects of our data protection obligations.
- Provides advice to services completing Data Protection Impact Assessments (DPIAs), Information Sharing Agreements, Privacy Notices etc
- Acts as a contact point for the ICO
- Supports the SIRO & Caldicott Guardian to complete their duties
- Is easily accessible and acts as the main point of contact for our employees, individuals, the ICO and data subjects

7 Personal data in the public domain

7.1 The council holds certain information about people in the public domain, for example planning applications are published on our website. Personal data classified as being in the 'public domain' refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the data subject.

7.2 The names and contact details of employees at service manager and above may also be made publicly available.

8 Responsibilities of staff and contractors

8.1 Staff and contractors must:

- complete the GDPR training as soon as they join the council, this is a mandatory requirement
- complete an annual refresher course available via the Learning and Development portal
- ensure that they only ever process personal data in accordance with requirements of the

Data Protection Act 2018

- follow the seven principles highlighted above
- follow the guidance provided by the Information Governance team on the intranet
- seek help and advice from the Information Governance team when required by emailing dataprotection@luton.gov.uk or calling extension 7700

9 Data security

9.1 Keeping personal data properly secure is vital in complying with the Data Protection Act. All staff and contractors are responsible for ensuring that any personal data they have access to be kept securely.

They are also responsible for ensuring that personal data is not disclosed inappropriately (either orally or in writing or accidentally) to any unauthorised third party.

9.2 This includes, as a minimum:

- always keep your passwords safe and never share them, follow the guidance on creating safe passwords
- secure any personal data kept in paper format in a lockable cabinet or pedestal, do not leave documents on your desk unattended at any time
- if you have to take hard copy documents out of the office make sure that you look after them at all times, this includes note books and files, consider whether you need to take files out of the office at all or if you can take them on an encrypted handheld device or laptop
- if you need to put hard copy data on a disc or memory stick make sure that the device that you use is encrypted and that the data is password protected
- if you have access to these devices make sure that they are stored securely and locked away safely when not being used

10 Sending personal data securely

10.1 You can send documents containing personal data securely using the following methods:

Email
This is the council's preferred method. Scan a copy of the file and move it to a secure location on the network. Send the file by secure data transfer (currently Egress). Ask the data subject to confirm receipt of the documents as soon as possible.

Hard copy
Documents should be hand delivered to the data subject wherever possible. Check ID and address for sending before handing over documents. Make sure that the documents are securely contained in a sealed envelope.

If it not possible for the data subject to collect the documents themselves, use the special delivery service and include the name of the data subject on the envelope to ensure that they sign for the documents.

Note: only sensitive personal data needs to be sent by special delivery. General correspondence like council tax bills can be sent via normal post. If you are unsure of the requirement, please email dataprotection@luton.gov.uk for advice.

Note: Check you have the correct address before posting.

Encrypted device
Where the data is especially sensitive you may want to consider saving the documents on a password protected, encrypted memory device rather than posting hard copies. You can send the password to the data subject once they have received the device by post to ensure that only they have access.

11 Data breaches

11.1 Occasionally things will go wrong and mistakes will be made. Sometimes this may entail significant financial or reputational risk for both Luton Council and our residents. It is vital that we can identify, evaluate and contain data breaches as soon as they occur.

11.2 Identifying data breaches quickly and effectively to limit any impact on our customers is critical to our success. Equally we need to understand where there are areas of weakness within our operating processes and continuously improve to reduce the risk of significant control failures leading to data breaches.

11.3 If an employee suspects a data breach has occurred they should report this to their line manager or the next most suitable colleague immediately. A data breach report should be completed as quickly as possible and as a maximum within 24 hours. The data breach report form can be found on the intranet.

Further guidance on managing data breaches effectively can be found on the staff Intranet or by contacting dataprotection@luton.gov.uk

12 Data subject rights

12.1 Data subjects have defined rights over the use of their data. These rights have been reinforced and extended by the Data Protection Act 2018. These rights are as follow.

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 Data Protection Act 2018.
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this ‘privacy information’.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than 28 calendar days.

Access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have 28 calendar days to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

- For more info on subject access requests go to the Subject Access Request page on the intranet.

Rectification

- The Data Protection Act 2018 includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have 28 calendar days to respond to a request.
- In certain circumstances you can refuse a request for rectification. Seek help from dataprotection@luton.gov.uk if you want to refuse a request to rectify data

Erasure

- The Data Protection Act 2018 introduces a right for individuals 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 28 calendar days to respond to a request.
- The right is not absolute and only applies in certain circumstances.

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, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have 28 calendar days to respond to a request.

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 easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- This only applies to information the data subject has provided to us and where we are using their consent to process information about them. If our systems do not allow us to transfer the data to another service automatically then we are required to provide copies of the information we hold so that they can transfer it over.

Object

- The Data Protection Act 2018 gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies you may be able to continue processing if you can show that you have a compelling reason for doing so.
- You must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- You have 28 calendar days to respond to an objection

Automated decision making and profiling

The Data Protection Act 2018 has provisions on:

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

The Data Protection Act 2018 applies to all automated individual decision-making and profiling. The Act has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

You can only carry out this type of decision-making where the decision is either:

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

If you are carrying out any of these activities you 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

12.2 The above rights are conditional depending on the reason we hold the data and why we may need to retain it.

12.3 Where we have a legal obligation to collect and process data or we are collecting the data to carry out a public task, the data subject's application to object to that data processing might be rejected.

This is because the council has a legal obligation under the law to keep certain data without the data subject's consent. For example, under the Local Government Finance Act 1992 and Local Government Finance Act 2012 we have to collect Council Tax and therefore have a legal obligation to collect certain data in order to comply with our duties.

12.4 Another example is where an individual claims that there is an error in the recording of a child protection meeting. In these circumstances it is unlikely that our records will be amended.

This is because the minutes will often contain the professional opinion of a social worker or other professional. Whilst we would not amend the original record we should place the individual's objections on file next to the original minutes so that these could be referred to as required.

12.5 However, when we rely on consent to process data about an individual we will, in most cases, be obliged to apply the above rights.

13 Prohibited activities

13.1 The following activities are strictly prohibited when processing personal and special category data:

- sharing passwords to access data
- leaving passwords unattended

- sending personal data to your personal email address to work on at home
- sending data to unauthorised personnel, always check that the recipients are authorised to view the information you are sending
- sending personal data in an insecure format
- losing or misplacing personal and sensitive data
- leaving personal data unprotected
- accessing information about a resident or member of staff where you do not have a legitimate reason for doing do
- taking unauthorised copies, or images of data for use outside of the council's permitted remit such as photocopies or screen shots of documents
- accessing personal data about an individual for your own personal use
- disclosing personal data to a third person outside of the council without a lawful basis

13.2 This data protection policy forms part of all employees' terms and conditions of appointment. Any breach of this policy will therefore be dealt with under the council's agreed disciplinary procedures, and may, subject to the seriousness of the breach, lead to a dismissal from the council's service.

14 Data protection by design and default

14.1 We shall implement appropriate organisational and technical measures to uphold the principles outlined in the Data Protection Act 2018. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

14.2 We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

14.3 Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist.

14.4 All new systems used for data processing will have data protection built in from the beginning of the system change.

14.5 We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

14.6 In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

14.7 Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

The UK GDPR defines pseudonymisation as:

"…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional

information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. However, the information required to tie the reference number back to an individual must be held separately.

For more information please see the ICO's webpage on personal data.

15 Data Protection Impact Assessments (DPIA)

15.1 You must do a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people
- process special category data or criminal offence data on a large scale
- systematically monitor a publicly accessible place on a large scale
- use new technologies
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit
- carry out profiling on a large scale, including evaluation or scoring of individuals
- process biometric or genetic data
- combine, compare or match data from multiple sources
- process personal data without providing a privacy notice directly to the individual
- process personal data in a way which involves tracking individuals' online or offline location or behaviour
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them
- process personal data which could result in a risk of physical harm in the event of a security breach

15.2 You must consider completing a DPIA when you identify:

- automated decision-making with significant effects
- systematic monitoring
- processing of sensitive data or data of a highly personal nature
- processing on a large scale
- processing of data concerning vulnerable data subjects (including children)
- innovative technological or organisational solutions
- processing involving preventing data subjects from exercising a right or using a service or contract

16 International transfers

16.1 The Data Protection Act 2018 imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter 5 of the GDPR.

16.2 You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

16.3 Adequate safeguards may be provided for by a legally binding agreement between public authorities or bodies or the transfer is:

- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register)

17 Exemptions

17.1 Exemptions to the Data Protection Act 2018 can apply in a small number of areas and only where the restriction respects the essence of the individual's fundamental rights and freedoms and it is a necessary and proportionate measure in a democratic society to safeguard either:

- national security
- defence
- public security
- the prevention, investigation, detection or prosecution of criminal offences
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security
- the protection of judicial independence and proceedings
- breaches of ethics in regulated professions
- the protection of the individual, or the rights and freedoms of others
- the enforcement of civil law matters

18 Conclusion

18.1 Compliance with the Data Protection Act 2018 is the responsibility of all members of staff, contractors and partners. Any questions about this policy or any queries concerning data protection matters should be raised with the Information Governance team at dataprotection@luton.gov.uk

19 Definitions

Subject Access Request or SAR
A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, certain exemptions may apply. Please refer to the SAR policy for further information

Freedom of Information Request (FOI) or Environmental Information Regulations (EIR)
A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may

be processed under this legislation. Please refer to the FOI policy for further information.

A request for access to data held about the environmental is dealt with under the Environmental Information Regulations 2004.

Personal Data
Personal data is data that relates to a living individual who can be identified directly or indirectly from the data.
Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Examples of personal data are the name and address of an individual; email and phone number; a Council Tax reference number or an NHS number.

Special Category Data
Certain types of personal data are given special protections under the Act because misuse could create more significant harm to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Information relating to criminal activities or convictions is not special category data but must be treated with similar safeguards in place.

Special category data includes:

- race or ethnic origin of the data subject
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- whether they are a member of a trade union
- their physical or mental health or condition
- their sexual life
- sexual orientation
- biometrics (where used for ID purposes)
- genetics

Confidential Data
This relates specifically to data that is given in confidence or data which is confidential in nature and is therefore not in the public domain.

Some confidential data will also be personal data and/or special category data and therefore come within the terms of this policy. Staff working in social care and in management roles will handle confidential data regularly and must be careful not to disclose this information incorrectly.

Data Controller
The organisation which determines the purposes and the manner in which, any personal data is processed is known as the data controller. The Council is the data controller of all personal data used and held within each individual department. For our purposes the Chief Executive is the data controller.

Data Processors
Organisations or individuals who process personal data on behalf of the data controller are known as data processors. This includes suppliers which handle personal data on the Council's behalf.

Data Subject
A living individual who is the subject of personal data is known as the data subject. This need not be

a UK national or resident.

Lawful Basis
These are the grounds specified by the Regulations which need to be satisfied for any data processing to be lawful. One condition needs to exist for processing personal data. Where special category data is processed a second condition must also exist.

Data Breach
A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A data breach may occur by accidentally sending an email to the wrong person or leaving a file in a public place. Breaches which result in a high risk of harm to the individual must be reported to the ICO within 72 hours.