LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

DATA PROTECTION AND PRIVACY POLICY & PROCEDURES

Document Control

Approved By:	Senior Leadership Team	**Date:**	08/07/2025
Document Location:	[redacted]		
Document Owner:			
Review Period:	Every 2 years unless significant changes to legislation		
Next Review Date:	July 2027		

Revision History

Version	Date	Reviewed By	Amendment Details
0.1	20/11/2017	[redacted]	Initial Draft
0.2	08/02/2017		Various amendments & tailoring to LCC
0.3	19/03/2018		Various amendments
0.4	27/03/2018		References
0.4	20/08/2022		None
0.5	04/07/2025		Various Amendments

CONTENTS

1 Introduction

This policy details how Lancaster City Council protects and processes personal data, in order to ensure individuals' privacy rights are respected and meet the requirements of UK and EU data protection legislation. The principal pieces of relevant legislation are the European General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (DPA18).

The GDPR is about respect for individual privacy and the obligations on both organisations and their staff to ensure that personal data about individuals is not obtained or held without good reason, used in any manner that the individual would not anticipate, or disclosed to someone who shouldn't have access to it. The DPA18 implements, expands on and clarifies the GDPR in UK law.

The aim of this policy is to ensure that the Council only holds information about people which is necessary for our functions as a Local Authority, processes this information fairly and transparently, and restricts access to this information generally to a "need to know basis".

2 Consequences of not complying with the GDPR

In the event that there is a breach of the GDPR, penalties may include:

- a fine of up to €20,000,000 (£17,500,000)
- formal enforcement or reprimand by the Information Commissioner's Office which may dictate specific steps or actions that we are required to complete

Any breach of personal data may also:

- cause distress or harm to the individuals involved
- damage our reputation
- result in disciplinary action (up to and including employment termination)
- lead to criminal prosecution

3 Policy statement

Lancaster City Council is committed to protecting personal data and respecting individual privacy. We will at all times comply with data protection legislation, and in particular will:

1. Ensure that proper policies and procedures are in place to protect personal data
2. Ensure that all staff who handle personal data understand their responsibilities and receive appropriate training at least every two years
3. Ensure that our IT systems and physical security measures protect the confidentiality, integrity and availability of personal data
4. Inform individuals how we intend to use their personal data
5. Give people access to the data we hold about them if they request it (subject access), and uphold other data subject rights
6. Only share personal data with other organisations when appropriate, and do so in a safe and secure manner, putting in place information sharing agreements where regular sharing takes place
7. Ensure that all contracts with third parties processing personal data on our behalf include appropriate clauses governing how the data will be processed
8. Investigate any personal data breaches, and take appropriate action to ensure that damage is minimised and future breaches are prevented

9. Use Data Protection Impact Assessments to embed privacy considerations into all new projects

All staff are responsible for ensuring that the Council complies with this policy, and some staff have additional specific responsibilities, which are detailed below.

This policy should be read in combination with the Council's supplementary Information Governance Policy Framework policies and will be supported by the provision of guidance and training to managers and staff throughout the Council.

4 Objectives

Key objectives of this policy are to ensure that:

- The Council is compliant with the letter and spirit of the law governing data protection
- Residents, customers, employees and other stakeholders trust the Council with their data
- Staff are confident in their ability to handle personal data appropriately, and know who to contact if they have any queries
- Any risk associated with data protection and privacy compliance shall be formally recognised and incorporated into the Council's Risk Management process

5 Scope

This policy is part of the Lancaster City Council Information Governance Policy Framework. A list of related policies is available in **Appendix 1**.

This Policy applies to, but is not limited to:

- All staff, including temporary staff, contractors and third parties employed directly or indirectly by third party organisations (e.g. subcontractors)
- Elected members and other users (e.g. volunteers) who are not employees of Lancaster City Council but require access to Lancaster City Council information or information systems
- Any third parties who process personal data on behalf of the Council, including those involved in the design, development, provision or operation of networks, information systems or services
- Access to Council information from remote locations where the computer and network facilities are not under the control of Lancaster City Council (e.g. working from home)

6 The GDPR

The GDPR regulates how we process personal data:

- **Personal data** is any information relating to any living person (the **Data Subject**) who may be identified from that or associated data
- **Processing** covers anything we might do with data, from its collection or creation, through to how it is stored, all actions performed with it and how it is disposed of when we no longer require it

The GDPR also covers a subset of personal data, **Special Category Data**, which is subject to additional restrictions under the GDPR and must be handled with additional care and security. This includes:

- data revealing racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying an individual
- data concerning physical or mental health, sex life, or sexual orientation

Data relating to criminal convictions or offences (including alleged offences, and proceedings for any offence) should also be considered particularly sensitive, and is subject to similar restrictions.

The GDPR sets out **Data Protection Principles** which we must always abide by when processing personal data. These principles say that:

1. Data must be:
    a. Processed lawfully, fairly and in a transparent manner
    b. Collected and processed only for specified and lawful purposes
    c. Adequate, relevant and limited to what is necessary for the purposes
    d. Accurate and kept up-to-date
    e. Held for no longer than necessary
    f. Protected by appropriate and effective security
2. Organisations must be responsible for and able to demonstrate compliance with the above

The Council can be subject to enforcement action (including fines) for a breach of any of these principles.

7 Compliance with the GDPR

7.1 Legal basis

The GDPR limits the circumstances under which data may be processed by specifying a number of conditions, at least one of which must be met in order for processing to be lawful. Prior to any data being collected, stored or used, it is important to identify which of these conditions applies. This will usually form a part of the DPIA process (see 7.6 below).

It will also be necessary to keep a record of the relevant condition as this will affect many of the obligations and subject rights associated with the data.

7.1.1 Consent

One of the conditions for processing is that the data subject has consented. However, due to the nature of the data processing undertaken by the Council it will *not* normally be appropriate to rely on consent in the majority of cases. As such, and because GDPR places additional requirements on us in respect of the consent process, other conditions should always be given precedence where possible.

Where it is absolutely necessary to obtain consent for processing, we should ensure the consent process meets the standards required by GDPR. In most cases the appropriate way to gather consent will be by the use of a yes/no tick box linked to a consent statement (and supported by

additional privacy information – see 7.2 below). In some cases, it may be necessary to split consent for different types of processing over multiple consent statements.

Where special category data is involved, it may also be appropriate to take additional steps to verify the identity of the data subject, such as requesting ID or obtaining a signature.

7.2 Privacy statements

In order for processing to be fair, individuals have a right to be informed how we will use their data. The Council meets this requirement through the use of Privacy Statements or Notices (previously known as Fair Processing Notices) both on our website and on any paper forms we use to collect data.

Staff should be aware of any Privacy Statements or Notices relating to their service area in case of enquiries from individuals about how their data is processed. The Council will provide printed copies of these notices to individuals on request.

7.3 Disclosures of information

There are many circumstances where the Council will need to disclose personal data to third parties, including individuals, other public authorities and other organisations. This could be on an ad hoc or regular basis. It is important that, prior to any disclosure, the full implications and legal basis have been considered – either on a case-by-case basis or (for regular disclosures) as part of an appropriate policy document or Data Protection Impact Assessment (see 7.6 below).

Where regular sharing between the Council and a third party organisation is proposed, it will be necessary to enter into an Information Sharing Agreement to ensure that both parties understand their rights and obligations.

Where requests to share information are received (whether ad hoc or on a regular basis), staff should contact the Information Governance Team if they are unsure whether the request should be met.

7.3.1 Disclosures for crime and taxation purposes

The DPA18 includes an exemption under Schedule 2, paragraph 2(1), allowing us to disclose information to third parties in any circumstances where this is necessary for:

- the prevention and detection of crime
- the apprehension or prosecution of offenders
- the assessment or collection of any tax or duty

Where requests to disclose information are received from the Police, HMRC, or other law enforcement bodies, these should – where possible – be made in writing specifying that the request is pursuant to Sch. 2, para 2(1) of the Act. However, where information is required as a matter of urgency we will try to assist without the need to make a written request first, though a retrospective confirmation will be required

In all cases a record will be kept of the request and the Council's decision whether or not to disclose the data.

7.3.2 Disclosures required by law or in connection with legal proceedings

The DPA18 includes an exemption under Schedule 2, paragraph 5(3), allowing us to disclose information to third parties in any circumstances where this is necessary for:

- The purpose of, or in connection with legal proceedings (including prospective legal proceeding)
- The purpose of obtaining legal advice
- The purposes of establishing, exercising or defending legal rights

Where requests to disclose information are received from others, these should – where possible – be made in writing specifying that the request is pursuant to Sch. 2, para 5(3) of the Act. However, where information is required as a matter of urgency we will try to assist without the need to make a written request first, though a retrospective confirmation will be required

In all cases a record will be kept of the request and the Council's decision whether or not to disclose the data.

7.3.3 References

All requests for references in respect of current or former employees should be dealt with by the relevant service. The Council should not provide references for an individual unless that individual has consented to the reference being given. Individual managers or staff should not provide references in their own name unless it is made clear that the reference is being made in their personal capacity and not as a representative of the Council.

7.4 Contracts

Where a third party is processing personal data on behalf of the Council, the GDPR stipulates that we ***must*** have a written contract in place covering data protection and information security. Where such contracts are being considered, managers should contact the Information Governance Team for guidance on appropriate contract terms.

Examples of relevant contracts include:

- cloud/hosting services
- contacting Council residents/customers (e.g. surveys, marketing, etc)
- providing services directly to residents on behalf of the Council (e.g. visiting customers at home, etc)

7.5 Individual rights

A Subject Access Request (SAR) is a written request made by or on behalf of an individual for the information the Council holds about them. The request does not have to be in any particular form and may be separate or connected to other communications (e.g. part of a complaint). Once we have received a request, we are required to respond to it within one month.

SARs are handled centrally, and anyone receiving a request should forward it to the Information Governance Team. The Council also has a separate Subject Access Request Policy which can be accessed on the staff intranet.

Individuals have a number of other rights under GDPR, including:

- the right to request that inaccurate information be rectified

- the right to have their data erased in certain circumstances
- the right to restrict all processing of their data if there is a dispute about how it is processed
- the right to object to certain types of processing

Any requests to exercise these rights should also be referred to the Information Governance Team.

7.6 Data protection impact assessments (DPIA)

A DPIA is a systematic consideration of all of the risks to individual privacy and to the Council which may arise from a project or process. In order to ensure that privacy and data protection compliance is built into all processes from the early stages of implementation ("privacy by design"), a DPIA will be considered for all new projects or significant changes to processes/procedures.

The Council has a separate DPIA policy, and template DPIA which can be accessed on the staff intranet.

7.7 Personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In the event of a breach, the Council has a Data Breach Management Policy which can be accessed on the staff intranet.

All staff should be aware that if a data breach occurs, it should be reported to the relevant Information Asset Owner (via your line manager if necessary), the Information Governance Manager, and if the breach occurs out of hours, the Duty Emergency Incident Officer.

7.8 Retention and disposal

It is important to ensure that personal data is not retained longer than necessary. This means that once we are no longer legally required to retain data, we should consider carefully whether or not it is needed for operational reasons, and dispose of it securely if not.

The Council has a separate Retention & Disposal policy which can be accessed on the staff intranet, and individual departments should keep a schedule of standard retention periods for all data they hold.

8 Other legislation and guidelines

8.1 CCTV policy and Code of Practice

Under the Protection of Freedoms Act 2012, the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by GDPR.

The Council has a separate CCTV policy (which can be found on the staff intranet) which complies with the Biometrics and Surveillance Camera Commissioner's Code of Practice on compliance with legal obligations under GDPR.

8.2 Direct marketing

Direct marketing means any marketing which is directed to individuals. This includes targeted letters, emails, phone calls and social media messages. The definition of "marketing" in this context is broad and not limited to promotion of products or services for sale – for example an email newsletter may be considered direct marketing under the legislation.

In most cases the Council will need consent to send marketing materials (see 7.1.1 above).

Early contact should be made with the Information Governance Team where any direct marketing campaigns are being planned.

9 Roles and responsibilities

The Council is a Data Controller under GDPR, which means that ultimately the Chief Executive and Management Team are accountable and responsible for compliance with the legislation. However, day-to-day matters relating to data protection will be dealt with by the Information Governance Team.

All staff are responsible for compliance with the legislation, this policy, and any other policies relating to data protection which are relevant to their work. However, the following roles carry specific data protection responsibilities.

9.1 Senior Information Risk Owner (SIRO)

Management Team will appoint one of its members as SIRO. The SIRO has overall responsibility and accountability for any risks associated with the use of personal information, and should ensure that individuals within the organisation comply with this policy, together with legislation and guidance relating to best practice.

The SIRO is also responsible for ensuring that an effective structure to monitor Information Governance and Information Asset Management is in place throughout the organisation.

The Deputy SIRO is the Information Governance Manager.

9.2 Information Governance Manager (IGM)

The IGM is responsible for advising all Council staff on the requirements of this policy and related legislation, producing any documents required at a corporate level for compliance with this policy and related legislation, and monitoring the Council's overall compliance with the legislation.

The IGM also has responsibility for the content of this Policy, ensuring its implementation, and instigating revisions in response to changing legislation and guidance, or a minimum every 24 months.

9.3 Information Security

All staff are responsible for ensuring that policies and procedures designed to keep information secure are followed, and Information Asset Owners (see 9.4 below) should ensure that appropriate procedures are implemented in their own service areas.

However, two key aspects to ensuring the security of information held by the Council are the security of the Council's network, and the physical security of Council buildings. Overall responsibility for these aspects specifically lies with the ICT Manager and the Facilities Manager respectively.

9.4 Information Asset Owners

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. A database containing personal information

is a clear example of a single information asset. Information assets have recognisable and manageable value, risk, content and lifecycles.

Senior managers (i.e. members of the Council's Leadership Team) assume the overall role of Information Asset Owners (IAOs) for the information assets in their service area. This means they are accountable for ensuring that their information assets are managed in line with the requirements of this policy and related legislation.

The IAO role profile details specific asset management responsibilities. IAOs may delegate these responsibilities to appropriate staff (e.g. system administrators) in their department. However, they should maintain an overview and understanding of the risks and privacy obligations which arise from data processing within their department.

The IAO role profile, and a list of current IAOs is available on the staff intranet.

9.5 IG/Cyber/ICT User Group

The IG/C/ICT group has been appointed to oversee Data Protection compliance within the Council and any employee should feel free to discuss with any member of the group any concerns they have about data held by the Council. Members of the user group are selected because they are in such positions in the Council that have the ability and authority to make strategic decisions. Their main role is to give strategic direction and support the SIRO and Information Governance Manager.

Membership details, Terms of Reference and minutes for the user group are available upon request from the IGM or ICT Projects and Security Manager.

10 Training and awareness

Data Protection and Privacy training forms part of the induction training and mandatory training programme for all Council staff. All staff will receive appropriate, approved training for their role. Refresher training will be mandatory for all staff.

A central record will be kept of all Information Governance and Data Protection training carried out.

The Council has a Privacy Training Plan (available on the staff intranet) which aims to improve awareness of Data Protection and Privacy legislation and best practice around the Council, and train key staff in specific issues relevant to their roles.

Appendix 1: Key Related Legislation & Policies

The below table lists the main legislation and internal policies relevant to the Council's handling of personal data.

Legislation	Council Policies
• General Data Protection Regulation 2016/679 (GDPR) • Data Protection Act 2018 • Freedom of Information Act 2000 • Environmental Information Regulations 2004 • Privacy and Electronic Communications Regulations (EC Directive) 2003 • Protection of Freedoms Act 2012	• Subject Access Request Policy • Data Protection Impact Assessment Policy • Data Breach Management Policy • CCTV Policy • Body Worn Video Policy • Information Security Policy • Records Management & Retention Policy

Appendix 2: Checklist to ensure Compliance with the GDPR

This Appendix contains prompts for some questions you may need to ask when considering how to comply with the GDPR. If you are still unsure about anything, you should check the Information Governance pages on the staff intranet or contact the Information Governance Team for advice.

Question	Which means:
1) Can you identify a living person through the data?	If **yes**, the data is personal data, and you must comply with the Act and this policy when processing the data. If **no**, can you cross-reference this data to other information which you hold or may be able to access, and does this then enable you to identify a living person (note: this includes numeric identifiers such as Vehicle Registration Numbers and IP addresses, even if the likelihood of cross-referencing is minimal)? a. If **yes**, then the data is personal data, and you must comply with the GDPR and this policy b. If **no**, then the data is not personal data within the definition of the GDPR, and this policy does not apply. Any new project involving personal data should involve a Data Protection Impact Assessment (DPIA). See the Council's DPIA policy on the staff intranet.
2) Is the data "special category data"?	Examples of such data are those which relate to race, political opinion, religious belief, membership of trade unions, physical or mental health or condition, sexual life, the carrying out of, alleged carrying out of, or proceedings relating to any criminal offence. If **yes**, then the conditions imposed on storage and processing of personal data must be most stringently adhered to – no more data than is strictly necessary is to be held, data is to be held securely, access to data is restricted to only that which is essential for the specified purpose for processing. Complete a Data Protection Impact Assessment.

3) Have you defined a specific purpose for using the data?	**Before** you collect any personal data: • ensure that you have a specific legal purpose for doing so (e.g. consent, legal requirement) • ensure that the data you intend to collect is sufficient, adequate, relevant and not excessive in relation to the intended purpose **At the time** that the personal data is being collected, notify the individual of the intended purpose for processing the data and (if appropriate) obtain their consent for this use of their data.
4) Are you intending to use personal data we already hold for new purposes?	**Before** using the personal data for a new purpose, ensure that this new purpose is consistent with the existing purpose for which we hold that data. Are the two compatible? ○ If not, then you may need to seek permission from the people whose personal data it is in order to use their personal data for the new purpose. **Note:** If the data is "sensitive personal data" then you will usually need the individual's explicit consent to use it for a new purpose – this should cover the specific processing details, the type of information (or even the specific information), the purposes of the processing, and any special aspects that may affect the individual, such as any disclosures that may be made. Note also that valid consent may subsequently be withdrawn.

5) Do you comply with "the conditions for processing" of personal data?	Has the individual given their consent to the intended processing of their personal data (taking into account the conditions for consent in the GDPR)? ▪ If **yes**, then processing the data is compliant with the Act ▪ If **no**, then have any one of the following conditions for processing been met? o The processing is necessary: ▪ In relation to a contract which the individual has entered into; or ▪ Because the individual has asked for something to be done so they can enter into a contract. o The processing is necessary because of a legal obligation that applies to the Council (except an obligation imposed by a contract) o The processing is necessary for exercising statutory functions If **yes** to any of the above conditions, then processing the data is in compliance with the GDPR. If no, you should contact the Information Governance Team to ensure that the processing is lawful.
6) Do you comply with the conditions necessary with respect to processing of "special category data"?	You must comply with "the conditions for processing" outlined in (5) above, **and, in addition**, with at least one of the conditions specific to special category data – which include: o The individual whom the sensitive personal data is about has given explicit consent to the processing (preferably in writing, in either paper or e-mail format) o The processing is necessary so that you can comply with employment law o The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals If **yes** to any of the above conditions, then processing the data is compliant with GDPR. If no, you should contact the Information Governance Team to ensure that the processing is lawful.

7) Do you have processes which ensure that the data is accurate?	▪ Have you taken reasonable steps to ensure the accuracy of any personal data you obtain? ○ You cannot always rely on the person to whom the data relates to be responsible for the accuracy of the data ▪ Have you ensured that the source of any personal data is clear? ▪ Have you considered any challenges to the accuracy of the information? ▪ Have you considered whether it is necessary to update the information? ▪ Where the data needs to be kept up-to-date, do you have processes in place to ensure that this happens?
8) Have you documented a retention and disposal policy for personal data - when and how is the data to be disposed of?	You need to ensure that personal data is not kept for longer than is necessary to achieve the purpose(s) for which it was collected. It is good practice to regularly review the personal data you hold, and delete anything you no longer need. Information that does not need to be accessed regularly, but which still needs to be retained, should be safely archived or taken offline.

9) Have you implemented appropriate security measures with respect to personal data?	▪ Personal data must be held and processed securely ▪ Ensure that the data is used and disclosed only in compliance with the defined purpose(s) for which the data is held ▪ Access to the data should be restricted to those people who need to process the data for its defined purpose(s) and for ensuring compliance with GDPR (for example, ensuring that the data is up-to-date) ▪ If processing includes transfer of data, then this should be done securely with the personal data encrypted in transit ▪ If personal data is accidentally lost, altered or destroyed, you should be able to recover it to prevent any damage or distress to the individuals concerned ▪ Security must be appropriate to ○ the nature of the information in question ○ the harm that might result from its improper use, or from its accidental loss or destruction, and ○ the risks to which the Council is exposed ▪ You will need to assess your information risk – you should review the personal data you hold and the way you use it to assess how valuable, sensitive or confidential it is, and what damage or distress could be caused to individuals if there were a security breach ○ Appropriate security needs to incorporate: ▪ physical ▪ technological ▪ management ▪ organisational aspects ○ Technological aspects do not need to be state-of-the-art and a trade-off is recognised between technical safeguards and cost, but the security needs to be appropriate for the type of data.

10) Can the rights of individuals be met with respect to personal data you hold for them?	• Upon making a written request (called a subject access request), the individual has a right to:
	  ○ a copy of their personal data
	  ○ a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
	  ○ details of the source of the data (where this is available)
	  ○ (in certain circumstances) a copy of the data in a reusable form (e.g. as a spreadsheet)
	
	• You may need to verify the identity of a requester – proof of identity – that they are the person whose data they are requesting to see
	
	• If you use a data processer, that is, an external person or company, to whom you pass personal data and who processes that data on your behalf – then you need to make sure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you or to the data processor
	
	• The individual also has rights to:
	  ○ have inaccurate data rectified
	  ○ have their data erased
	  ○ restrict processing of their data if there is a dispute about how it is processed
	  ○ object to processing
	  ○ object to automated processing, including profiling, and obtain human intervention
	
	(None of these rights are absolute, and so there may be circumstances where they do not apply in full)

11) Is personal data being sent to a third party who will be holding and/or processing that data?	If yes, then the Council is still legally responsible for how and why the data will be processed by the third party. The Council must ensure that any processing of personal data for which they are responsible complies with the Act. ▪ A formal contract must be in place between the Council and the third party which stipulates where and how the data is to be processed. o Special security considerations need to be made where data is transferred outside the United Kingdom ▪ Where you transfer data to a third party: o You must see if it is necessary to transfer personal data – can the data be made anonymous? If personal data must be sent, then: ➢ You must choose a data processor that provides sufficient guarantees about its security measures to protect the processing it will do for you ➢ You must take reasonable steps to check that those security measures are being put into practice ➢ There must be a written contract setting out what the data processor is allowed to do with the personal data. The contract must also require the data processor to take the same security measures you would have to take if you were processing the data yourself ▪ The Council must have in place effective means of monitoring, reviewing and auditing the processing of personal data by the third party.
12) What is the policy in the event that a breach of security occurs affecting personal data?	Report the breach to the Information Governance Team, the relevant Information Asset Owner, and (if the breach occurs out of hours) the Duty Emergency Incident Officer (via Emergency Control). See Guidance on Data Breach Incident Management on the staff intranet.