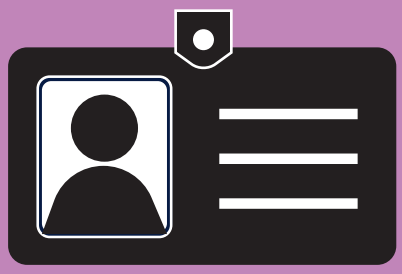
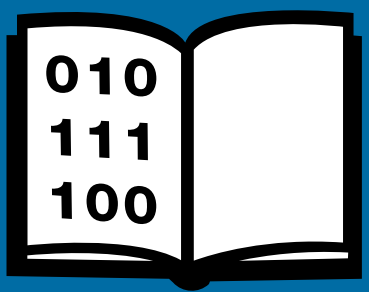
CARLISLE CITY COUNCIL

www.carlisle.gov.uk

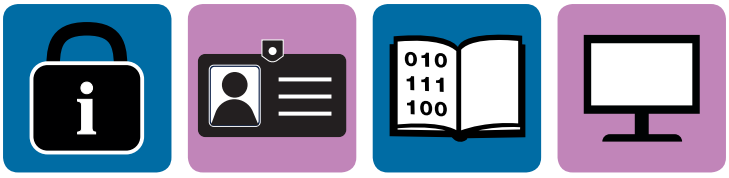
Carlisle City Council

Data Protection Policy





Contents



1. Introduction

Carlisle City Council ("the Council") needs to create, collect, use, share, retain and destroy personal data to comply with its legal obligations, undertake its statutory duties and to deliver services required or requested by individuals. The processing of personal data is key to achieving these objectives and the Council must ensure that all processing is appropriate and safely managed.

The Council regards respect for the privacy of individuals and the lawful and careful treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it interacts with. To this end, the Council is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation and other related legislation. The Council will ensure that it treats personal information lawfully and proportionately.

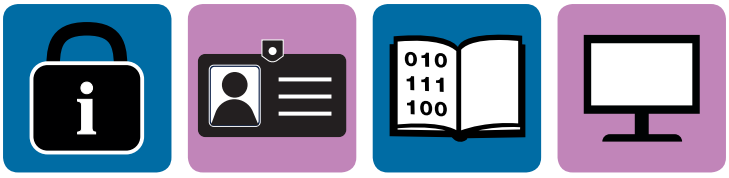
This Policy sits within the Council's Information Governance Framework which sets out the Council's overarching approach to the governance of its information and its commitment to embedding a Corporate culture of Information Governance.

2. Purpose

The purpose of this Policy is to set out the Council's principles, approach and commitment to the processing of personal data to achieve, demonstrate and maintain compliance with the General Data Protection Regulation[1] ("GDPR"). This will be achieved by ensuring:

- Personal data is valued and processed appropriately
- Relevant procedures and guidance are in place
- Appropriate organisation and technical security and protection measures are in place to guard against data breaches
- There is commitment to allocating key roles and responsibilities to those staff who process personal data
- There is regular mandatory training for staff and awareness raising
- Robust risk management in relation to the processing of personal data

1 General Date Protection Regulation ((EU) 2016/679)



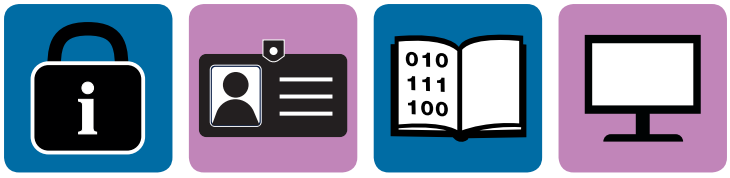
3. Scope

This Policy and associated procedures apply to all employees and Elected Members when processing personal information of which the Council is either the data controller or data processor. It will apply to third parties who are engaged to work with the Council, especially when they process personal data on the Council's behalf. Third parties whom the Council shares information with and those who request information from the Council will also need to consider and comply with this Policy in relation to the personal data they receive from the Council.

4. Objectives

The objectives of this Policy are to:

- Ensure compliance with the GDPR by committing to:
  - The rights of individuals
  - The protection of information
  - Adhering to the GDPR principles
  - Developing and implementing adequate procedures
  - Undertaking appropriate risk assessment
  - Undertaking audits
  - Implementing appropriate records management practices
- Manage and prevent the occurrence of data breaches
- Ensure the Council's approach to data protection is open, transparent and accessible to individuals
- Safeguard the rights and freedoms of individuals



5. Key Definitions

Personal Data

This is data which relates to a natural living individual ("data subject") who can be identified directly or indirectly from that data or through additional information which is or could be accessible.

This includes the name, address, telephone number, national insurance number as well as any expression of opinion about the individual, and any indication of the intentions of the data controller or any other person in respect of them.

Special Category Data

This is personal data consisting of information as to any of the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life
- Sexual orientation

Special category personal data is subject to much stricter conditions of processing.

Processing

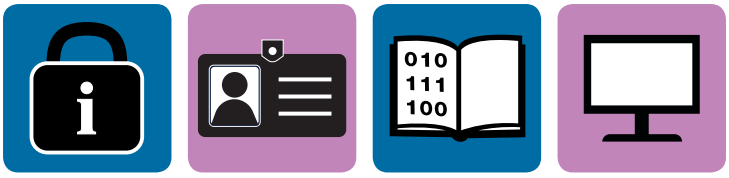
The definition of processing covers everything from creating, collecting, using, sharing, retaining and destroying personal data.

Data Controller

A Data Controller is a person or organisation who decides how any personal data will be held and processed, and for what purposes. The Council is a Data Controller.

Joint Data Controllers

These are people or organisations (for example, the Council, NHS Cumbria or Cumbria Constabulary) who jointly process and share information.



Data Processor

A data processor is a person or organisation who processes personal data on behalf of a data controller. For example, when the Council is a data controller, a supplier, contractor or agent will be contracted to process personal data on its behalf.

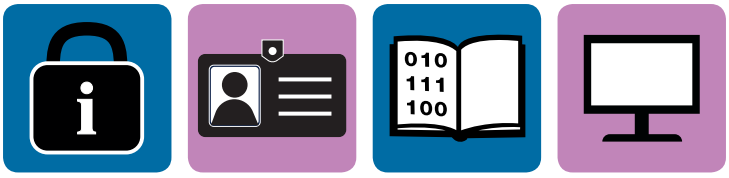
In some circumstances, the Council is a data processor.

For other applicable definitions, please refer to the GDPR and related guidance.

6. Data Protection Principles

The General Data Protection Regulation sets out six principles for the processing of personal data which are legally binding on the Council. Personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. 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.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. 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.
5. 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 General Data Protection Regulation in order to safeguard the rights and freedoms of the data subject.
6. 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.



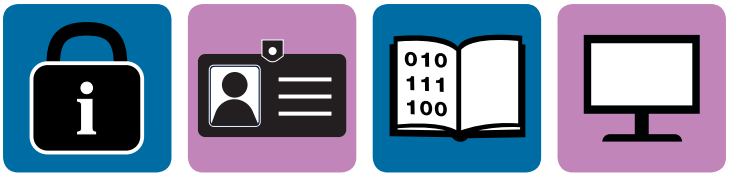
7. Lawful Bases for Processing Personal Information

The lawful bases for processing are set out in the General Data Protection Regulation. At least one of these must apply whenever the Council processes personal information:

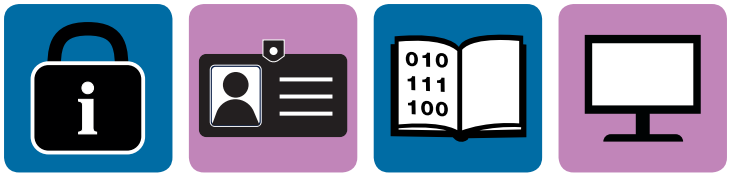
- Consent: the individual has given clear consent for the Council to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract that the Council has with the individual, or because the individual has asked the Council to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for the Council to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public interest: the processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council.
- Legitimate interests: the processing is necessary for the purposes of legitimate interests pursued by the Council or a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by the Council in the performance of its official tasks: it can only apply to the Council when it is fulfilling a different role.

To process special category data, one of the following must apply:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
- 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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- 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.



- 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.
- processing relates to personal data which are manifestly made public by the data subject.
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- 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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.
- 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.



8. Policy Statements

8.1. Privacy Notices

The Council will ensure it prepares and makes accessible compliant privacy notices which are clear, transparent and intelligible and, tailored to the relevant data subjects. It will ensure these are provided to data subjects at the point of data collection or, in the case that information is received from a third party, will make sure the privacy notice is provided within 1 calendar month. The Council applies the endorsed 'layered' approach therefore the overarching privacy notice can be accessed by visiting https://www.carlisle.gov.uk/Privacy-Statement. For individual Service privacy notices, most will be available under the Service Privacy Notices Section, whilst key information will be included on application forms etc. which will then sign-post to the next level notice.

8.2. Consent

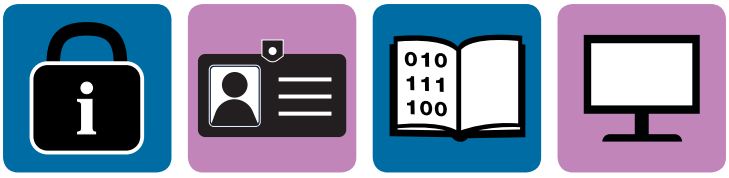
Consent, being one of 6 lawful bases for processing, provides individuals with full control over their personal data and the purposes for which it is processed. The Council as a local authority is limited in many respects to enabling individuals to provide their consent due to its various statutory duties and obligations. However, the Council is committed to seeking appropriate consent in relevant circumstances when individuals have free choice. The Council will ensure that consent is informed, freely given and unambiguous. It will also make sure data subjects are aware of their right to withdraw consent and of how they are able to do this.

8.3. Rights of individuals

The Council is committed to ensuring individuals' rights are respect and adhered to. The Council will make sure it's privacy notices include the rights of individuals and the details of how they can submit requests to the Council.

Individuals' rights under GDPR are:

- The right to be informed about how their information will be processed.
- The right of access to their personal information.
- The right to rectification, which is the right to require the Council to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Council processing their personal information.
- Rights in relation to automated decision making and profiling



8.4. Data Protection Impact Assessments

As required under the GDPR, the Council will undertake mandatory Data Protection Impact Assessments (DPIA) prior to carrying out processing which is likely to result in a high risk to individuals' rights and freedoms. It will further consult with the ICO in circumstances when it cannot mitigate against any high risks to individuals.

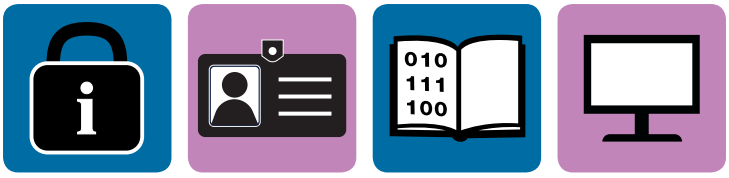
The purpose of a DPIA is to help identify and minimise the data protection risks of a project. The Council will undertake a DPIA in relation to all significant projects which require the processing of personal data and in particular, if we plan to:

- use systematic and extensive profiling with significant effects
- process special category or criminal offence data on a large scale
- systematically monitor publicly accessible places on a large scale
- use new technologies
- use special category data to decide on access to services
- process biometric data
- process genetic data
- match data or combine datasets from different sources
- collect personal data from a source other than the individual without providing them with a privacy notice
- track individuals' location or behaviour
- profile children or target services at them
- process data that might endanger the individual's physical health or safety in the event of a security breach

For existing processing activities which are likely to result in high risk, the Council will consider the need to undertake retrospective DPIAs based on previous efforts which have been made to consider and manage risk. Any significant changes to existing processing activities will require a DPIA to be undertaken, when the processing could result in high risk.

The Council's DPIA process and guidance has been designed to comply with the GDPR and both should be followed.

The information Governance Manager must be consulted in relation to all DPIAs.



8.5. Privacy by design

The Council's Privacy by design approach will be heavily linked to the Council's Data Protection Impact Assessment process and will also be embedded within other areas such as risk management, business planning, project initiation and Committee reporting.

The focus is on ensuring that privacy risks and concerns are identified from the project initiation stage and managed throughout the project lifecycle. This will be done by considering Information Commissioner and industry guidance on initiatives such as data minimisation and pseudonymisation.

8.6. Data Sharing

In order to meet its legal obligations, statutory functions and deliver services to individuals, the Council requires to share personal data in certain circumstances with third parties. For example, with NHS Cumbria or Cumbria Constabulary.

Data sharing will be undertaken in accordance with the GDPR and the Information Commissioner Office's Data Sharing Code of Practice. In addition, regular data sharing will be covered by an appropriate Information Sharing Protocol (ISP) and details will also be included in the Council's privacy notices.

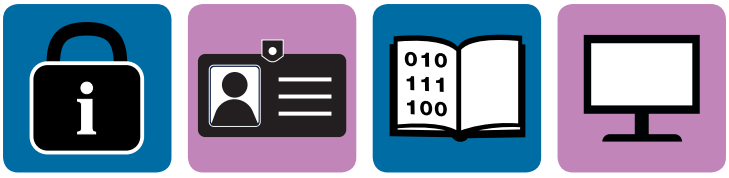
One-off instances of data sharing or third-party requests will be considered on a case by case basis in accordance with the legislation.

8.7. Data breaches

Data breaches which result in the accidental loss, disclosure, destruction of or damage to personal data can have significant impacts on individuals. The Council will take all reasonable organisational and technical steps to ensure the protection of the personal data it processes. Despite this, data breaches may still occur.

The Council has put in place a Data Breach Response Procedure to support and manage the response to any data breaches it experiences.

The Information Governance Manager must be notified of all data breach incidents and the Council's procedure must be followed. In the case of a IT security breach, the Council's ICT Services Manager will lead the response. Near miss incidents and allegations of data breaches should also be brought to the attention of the Information Governance Manager, to enable risk areas to be identified, lessons to be learned and to manage the risk of actual data breaches occurring.



The GDPR places an obligation on the Council as a data controller to report all data breaches which are likely to result in a risk to individuals to the ICO within 72 hours. The Council's procedure is designed to assist the Council in meeting this requirement.

Should a data breach occur which is likely to result in a high risk to individuals, the Council will also notify those individuals without delay.

For detailed guidance with steps to follow and a template response plan, please refer the Council's Data Breach Response Procedure.

8.8. Documentation

The Council will adhere to the GDPR requirements to ensure it keeps appropriate documentation to record its processing activities, data sharing instances and retention periods etc. The Council will also comply with any request from the ICO to make this available to them as and when required.

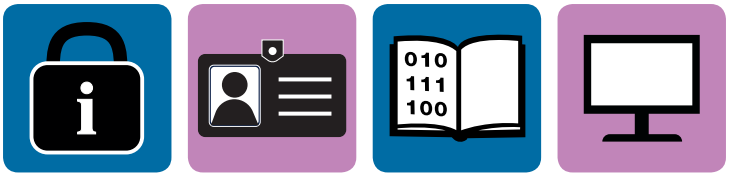
The Council will undertake information audits to identify its processing activities, keep records of this and, will aim to record this in an electronic format with all information appropriately linked.

8.9. Contracts

The Council is obliged under the GDPR to have in place written contracts with data processors such as suppliers, contractors or agents etc. which must contain, as a minimum, certain terms. The Council will ensure that it has the appropriate contracts and terms in place with its data processors and, that on occasions when it is a data processor, appropriate contracts are also in place.

A contracts guide has been prepared with standard clauses and guidance which sits with Legal Services who must be consulted with for all contracts.

To ensure the Council is able to make informed decisions about the organisations it selects as data processors on its behalf and, can evidence this to the ICO; a Data Protection Data Processor Compliance Questionnaire has been embedded into the procurement process and must be completed by any tendering organisation who will process personal information on the Council's behalf.



9. Roles and Responsibilities

Overarching roles and responsibilities in relation to Information Governance are contained within the Council's Information Governance Framework.

In addition to those overarching roles, the Council also has the following roles and responsibilities, specifically in relation to data protection:

Data Protection Officer

The role of the Data Protection Officer (DPO) is to:

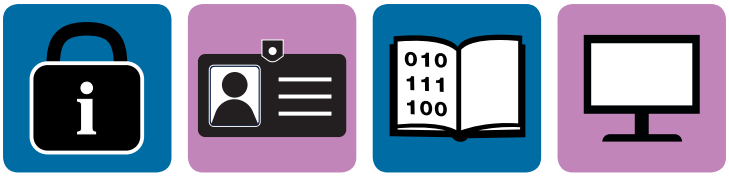
- Inform and advise the Council and its employees about their obligations to comply with the General Data Protection Regulation and other data protection laws.
- Monitor compliance with the General Data Protection Regulation and other data protection laws, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations and related audits.
- Provide advice about data protection impact assessments and monitor their performance.
- Act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.
- Support individuals with their rights under the General Data Protection Regulation.

The Council's DPO is the Information Governance Manager.

Corporate Information Officer

The role of the Corporate Information Officer is to:

- Administer and process subject access and broader data protection requests in conjunction with Council department contacts to ensure responses are handled appropriately and issued in a timely manner.
- Collate and distribute weekly reports summarising data protection requests received to elected members & Senior Management Team.
- Provide advice and assistance to requesters in order to discharge the responsibilities enforceable by the Information Commissioner.
- Ensure efficient operation of relevant filing systems and implementing changes as necessary.



10. Training, Communication and Awareness

Data Protection training is available in the form of mandatory e-Learning for all staff which is built into the Council's induction training programme. In addition, face-to-face training is also built into the Council's Governance training programme which is available to staff and Elected Members.

Data Protection training is mandatory for all staff and refresher training will be undertaken on a yearly basis to ensure awareness raising and knowledge development. Training materials will be reviewed on a yearly basis to take into account any legislative changes, industry and ICO guidance and, any areas of concern or risks to the Council at that time.

11. Implementation and Compliance Monitoring

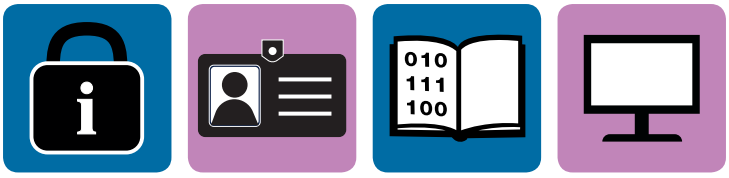
This Data Protection Policy will be implemented and supported by Directorates and teams and overseen and monitored by the Information Governance Manager.

New associated Procedures will be developed in collaboration with key subject matter experts, consulted through the Governance Sub-Group and the Senior Management Team, and signed off by the Corporate Director of Governance and Regulatory Services. They will subsequently be considered as applicable under this Policy and circulated to relevant staff for awareness.

Implementation and adherence of this Policy will be monitored by the Information Governance Manager who will carry out two-yearly audits to ensure it is applied in practice.

12. Associated Procedures, Guidance and Documents

- Privacy Notice Guide
- Record of Processing Activity
- Data Processing - Standard Contract Terms
- Data Protection - Data Processor Compliance Questionnaire
- Subject Access Request Procedure
- Data Subject Rights Procedure
- Third Party Requests Procedure
- Data Sharing
- Consent
- Data Breach Response Procedure
- Data Protection Impact Assessment Guide



13. Further Information and Guidance

Council's Data Protection Intranet Page Guide to General Data Protection Regulation (GDPR)

14. Review

This Policy will be reviewed two-yearly following the implementation and adherence audits which will inform the review.