# Data Protection Policy

Version 7.0, 03 May 2023

This is a controlled document. The digital PDF file published on InsideNL is the control copy.

- Always access this document from the control location.
- When you open this document, your device may automatically download it. If it does, you should still open it from the control location in future.
- You can print this document, but a printed copy isn't the control copy.
- Don't save any digital copies of this document anywhere. This includes your device, USB flash drives, network drives, OneDrive, Teams/SharePoint, or any other digital storage device, system, service, or location.

# Document control

| | | | |
|---|---|---|---|
| **Title** | Data Protection Policy | | |
| **Governance group** | Data Governance Board | | |
| **Owner** | Katrina Hassell, Senior Information Risk Officer | **Contact** | hassellk@northlan.gov.uk |
| **Author** | Collette Crainie, Solicitor (Information and Standards) | **Contact** | crainiec@northlan.gov.uk |

## Revision history

| Version | Originator | Review start date | Revision description and record of change |
|---|---|---|---|
| 7.0 | Collette Crainie | 03 May 2023 | Biennial review. |
| 6.0 | Paul Corrigan | 26 March 2021 | Biennial review. |
| 5.0 | Paul Corrigan | 30 April 2020 | Biennial review incorporating feedback from Data Governance Board and Data Management Team. |
| 4.0 | Gerry Gardiner | 10 May 2018 | To reflect the UK Genera Data Protection Regulations and Data Protection Act 2018. |
| 3.0 | Gerry Gardiner | 15 November 2016 | Biennial review. |
| 2.0 | Gerry Gardiner | 04 July2014 | Data Governance Board consultation. |
| 1.0 | Gerry Gardiner | 22 February 2013 | Data Governance Board consultation. |

## Document approvals

| Version | Governance group | Date approved | Date approval to be requested (if document still in draft) |
|---|---|---|---|
| 7.0 | Policy and Strategy Committee | | 08 June 2023 |
| 6.0 | Policy and Strategy Committee | 03 June 2021 | |
| 5.0 | Policy and Strategy Committee | 11 June 2020 | |
| 4.0 | Policy and Resources Committee | 07 June 2019 | |
| 3.0 | Policy and Resources Committee | 21 June 2017 | |
| 2.0 | Policy and Resources (Finance and Customer Services) Sub Committee | 16 September 2014 | |
| 1.0 | Policy and Resources (Finance and Customer Services) Sub Committee | 14 March 2013 | |

## Consultation record (for most recent update)

| | | |
|---|---|---|
| **Consultation status** | Stakeholders consulted between 15 March 2023 and 12 April 2023 | |
| **Stakeholders consulted and dates** | Business and Digital Management Team<br>Data Management Team<br>Data Governance Group<br>Technical Design Authority | 21 March 2023<br>15 March 2023<br>29 March 2023<br>21 March 2023 |

## Strategic alignment

**Plan for North Lanarkshire**

Improving the Council's Resource Base – A Workforce Strategy that is built around the needs of the council (as a single resource base) to deliver the priority outcomes, ensuring future workforce requirements, new skills and innovative approaches, and succession planning are recognised.

| Strategic alignment |
| --- |
| **Digital and IT Strategy**<br>The Digital and IT Strategy brings together separate but related plans and policies that contribute to the development and delivery of our digital vision. The Data Protection Policy is one of these. It supports the strategy setting out how we protect personal data using principles, rules, and guidelines to make sure we continue to comply with data protection laws. |

| Next review date | |
| --- | --- |
| **Review date** | |

# Contents

# 1. Introduction

To deliver services effectively North Lanarkshire Council (the council) needs to collect, process and hold large volumes of information which includes personal information (personal data) relating to current, past and prospective customers, clients, employees, workers, elected members, suppliers and contractors.

In addition, it may from time to time be required by law to process personal information to comply with the requirements of government departments and other public agencies. There are also instances where we process personal data for contractors and arms' length external organisations and third parties process council information which includes personal data.

**To deliver services effectively we need to collect, process, and hold large volumes of information relating to organisations and individuals. This includes personal data.**

# 2. Purpose

This Data Protection Policy sets out how we protect personal data to comply with data protection laws using:

- principles,
- rules, and
- guidelines.

# 3. Scope

This policy is applicable to all personal data held by the council whether in manual format via council information technology systems accessed either on council premises or via mobile or home-working equipment. Personal data held on removable devices and other portable media is also covered by this policy.

The policy applies to all employees, workers, elected members, clients, suppliers, third party contractors and any other individuals or organisations who access council information.

This policy is not part of the contract of employment and the council may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport, store and otherwise process personal data will adhere to the rules of the policy. Any breach of the policy by an employee will be taken seriously and may result in disciplinary action.

Elected members are required, in respect of their use of data, to comply with their obligations as set out in paragraphs 3.21 to 3.23, and 6.2 of the Councillors' Code of Conduct and paragraphs 70 to 82 of the associated Guidance. Members need to be aware of the potential for personal liability under the relevant legislation, in respect of both criminal and civil court proceedings as well as the imposition of fines by the Information Commissioner.

Guidance to organisations on the UK GDPR is available from the Information Commissioner's Office website.

# 4. Governance

This policy forms part of a suite of documents that are covered by the Digital and IT Strategy.

The **Policy and Strategy Committee** has **approval** authority for, and oversight of, this policy. The **Data Management Team** then the **Data Governance Board** – as **key stakeholders** – oversee its review and consider its contents before referring it on for approval. The **Chief Officer of Business and Digital** – as the council's Senior Information Risk Owner – is **accountable** for its governance. The **Data Protection team** is **responsible** for the following activities.

1. Produce, publish and promote this policy.
2. Give guidance on how to apply and comply with this policy through standards, procedures and guidance notes – see product set for list and links.
3. Review every two years, with other reviews when needed. For example, following a critical security incident, new legislation, a significant threat, an audit action.
4. Report to management teams, governance and working groups, committees and scrutiny panels.

# 5. Information risk

## The collation and holding of information of any nature creates a risk of information falling into the hands of third parties or misuse of the information. To manage those risks the council has in place a number of policies.

Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The council is exposed to potential fines of up to 20 million Euros (approximately £18 million) or 4% of its total annual turnover, whichever is higher and depending on the breach, for failure to comply with data protection law.

The **Senior Information Risk Owner (SIRO)** is the Chief Officer of Business and Digital. The SIRO's duty is in respect of all information collected, held and processed by the council. The SIRO is not a position prescribed or regulated by legislation. It is a position recommended by the Information Commissioner. The SIRO is responsible for:

1. overall information risk and they will provide written advice on a regular basis to the Chief Executive on internal control and performance in respect of information risk;
2. assessing the impact of information risks on the council and how the risks may be managed ensuring arrangements are put in place to mitigate risks. They will implement and lead information risk and management processes within the council; and
3. advising the Corporate Management Team on effectiveness of information risk management across the council.

# 6. Data protection

The UK General Data Protection Regulation (the UK GDPR) sitting alongside the Data Protection Act 2018 (the Act) make provision for how personal data (information) about living individuals in any form including paper and electronic must be collected, processed and held. They impose restrictions on how the council may process personal data, and a breach of the data protection laws could give rise to criminal and civil sanctions, including fines, as well as adverse publicity.

The legislation provides also that:

1. **special categories of personal data** (that is, data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data, data concerning health, sex life or sexual orientation); and
2. **personal data relating to criminal offences and convictions** shall only be collected and/or processed for certain specific lawful purposes.

The council can only process special categories of data and personal data relating to criminal offences and convictions where certain additional conditions apply. The council has produced an appropriate policy document for such processing.

- For details of conditions for processing special categories of personal data see Article 9 of the UK GDPR and Schedule 1 of the Act.
- For details of conditions for processing personal data relating to criminal offences and convictions see Article 10 of the UK GDPR and Schedule 1 of the Act.

# 7. Personal data

This policy adopts the definition of personal data contained in the UK GDPR.

1. Personal data is any information relating to an identified or identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier.
2. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.
3. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data.

4. Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.
5. Examples of personal data include:
    a. a name and surname;
    b. a home address;
    c. an email address such as name.surname@company.com;
    d. an identification card number;
    e. CCTV images of an individual;
    f. location data (for example the location data function on a mobile phone);
    g. an Internet Protocol (IP) address; or
    h. a cookie ID.
6. The following are examples of data which are not considered to be personal data:
    a. a company registration number;
    b. an email address such as info@company.com; and
    c. anonymised data.

# 8. The data protection principles

## The UK GDPR requires organisations which handle personal data to collect, process and hold personal and confidential information securely and responsibly. This includes destroying information safely when it is no longer required.

The UK GDPR sets outs the following key principles.

| GDPR principle | Description |
|---|---|
| **First: Lawfulness, fairness and transparency** | Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. |
| **Second: Purpose limitation** | Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. |
| **Third: Data minimisation** | Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. |

| GDPR principle | Description |
|---|---|
| **Fourth: Accuracy** | Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. |
| **Fifth: Storage limitation** | Personal data shall be 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. |
| **Sixth: Integrity and confidentiality** | Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against:<br>▪ unauthorised or unlawful processing, and<br>▪ against accidental loss, destruction or damage<br>using appropriate technical or organisational measures. |
| **Seventh: Accountability** | The council is also responsible for, and must be able to demonstrate compliance with, the principles. |

# 9. Discharging our responsibilities

## 9.1. The Controller

In terms of the legislation, the council will normally be the Data Controller. In some cases, the council may be acting as:

- a Joint Data Controller in conjunction with another organisation; or
- a data processor, for example, where it is providing services to an external or arms-length organisation and is processing information of which that organisation is data controller and under their instruction in connection with provision of that service.

To ensure compliance with the data protection principles, the council will:

1. Observe fully conditions regarding the lawful, fair and transparent collection and use of data.
2. Meet its obligations to specify the purposes for which data is used.
3. Collect and process appropriate data and only to the extent that it is required to fulfil operational needs or to comply with any legal requirements.
4. Ensure the accuracy of the data used.
5. Put in place arrangements to determine the length of time the data is held.
6. Take appropriate measures to keep the data secure.

## Compliance with the data protection principles

### 1. Lawful, fair and transparent obtaining and processing

The council may only collect, process and share personal data fairly and lawfully and for specified purposes. The law restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly, lawfully and without adversely affecting the data subject.

**Lawful basis**

- It is essential that the legal ground (lawful basis) being relied on for each processing activity is identified and documented.
- The lawful bases for processing personal information are as follows. At least one of these must apply when you process personal data:
  - → **Consent** – the individual has given clear consent for you to process their data for a specific purpose.
  - → **Contract** – the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
  - → **Legal obligation** – the processing is necessary for you to comply with the law (not including contractual obligation).
  - → **Vital interests** – the processing is necessary to protect someone's life.
  - → **Public task** – the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  - → **Legitimate interests** – the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).
- **For the majority of processing or personal data carried out by the council the public task condition will be the appropriate lawful basis**, however, it is very important that the appropriate lawful basis or bases are identified at the outset of processing activity and these will vary depending on the nature and circumstances of the processing in question.

**Special category data**

- For processing of special category data, a further additional lawful basis for processing requires to be satisfied. Special category data under data protection law relates to information about an individual's
  - → race or ethnic origin,
  - → politics,
  - → religion,
  - → trade union membership,
  - → genetics,
  - → biometrics (for ID purposes),
  - → health,
  - → sex life, or
  - → sexual orientation.

## Compliance with the data protection principles

- There are extensive lawful bases within Schedule 1 of the Act for processing in relation to special categories of personal data and data relating to criminal convictions. Advice should be sought from Legal and Democratic services in relation to proposed processing of such data.

**Using personal data**

- The council will be clear when **telling people how their personal information will be used**. This requirement to tell people will always apply, no matter how the information is gathered (for example, paper forms, email, surface mail correspondence, web data collection forms, or any other method). We must say clearly in all of these methods how we will process people's personal information.
- This should principally be achieved by the use of **privacy notices**.
- Privacy notices are a legal requirement. They inform data subjects about the collection and use of their personal data. This relates to the requirement under the legislation that processing of personal data should be transparent.
- Privacy notices should provide individuals with information about our purposes for processing their personal data, how long their data may be retained and with whom it may be shared. This information should be available to individuals at the point of collection of their data. The council's privacy notice can be found on our website.
- Services should develop their own privacy notices to provide more specific information in relation to particular categories of processing of personal data in relation to their functions. Privacy notices should be regularly reviewed and developed to ensure that they provide accurate and adequate information about the council's processing activity.

**Consent**

In many cases the council may process personal information without the **consent** of the data subject where this is required or permitted by law. However, the council will ask for an individual's **informed consent** if this is needed (the individual must understand what their information will be used for and how it will be shared and stored) (see first data protection principle). Unless the council can rely on another legal basis of processing, explicit consent will be required for processing special categories of personal data.

- An individual consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. The individual may be asked to sign or to tick a box to give their consent. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.
- Individuals must be easily able to withdraw consent to processing at any time and withdrawal must be promptly acted upon. Consent will need to be refreshed if the council intends to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.
- The council will need to evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

## Compliance with the data protection principles

### 2. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

- The council cannot use personal data for new, different or incompatible purposes from those disclosed when it was first obtained, unless consent is obtained or there is a clear obligation or function set out in law.
- Where information is used for a purpose other than for which it was obtained, privacy information should be updated accordingly to ensure data subjects are so aware.

### 3. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. The council:

- may only process personal data when required to do so in performance of its duties;
- cannot process personal data for any unrelated purposes;
- will not collect excessive data; and
- will ensure that any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, it should be deleted or anonymised in accordance with the council's data retention guidelines.

### 4. Accuracy

The council must make sure that all personal information that it holds is accurate and, where necessary up to date (see fourth data protection principle).

- Information should be reviewed regularly, and service managers must have procedures in place to make sure that inaccurate or out of date information is updated.
- Information which the council no longer needs to hold must be destroyed in line with the council's guidelines on Information Security.

### 5. Storage limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

- The council must not keep personal data in a form which permits the identification of individuals for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.
- The council will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held; unless a law requires such data to be kept for a minimum time.

## Compliance with the data protection principles

- The council will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the council's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.
- Individuals will be informed of the period for which data is stored and how that period is determined.

### 6. Security, integrity and confidentiality

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will continue to develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

Personal data may only be transferred to third party service providers who agree to comply with the policies and procedures required by the council and who agree to put adequate measures in place, as requested.

The confidentiality, integrity and availability of personal data must be maintained, that is –

- **Confidentiality**: only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity**: personal data is accurate and suitable for the purpose for which it is processed.
- **Availability**: authorised users are able to access personal data when they need it for authorised purposes.

### 7. Data processors

The law requires the council to put in place a written contract with each third-party data processor, which contract must meet specific minimum requirements, including procedures and policies to maintain the security of all personal data from the point of collection to the point of destruction.

Personal data may only be transferred to a third-party data processor if the processor agrees in writing to comply with those minimum requirements.

### 8. ICO assessments, audits, investigations and action

The council must co-operate with any data protection assessment, audit or investigation carried out or action taken by the Office of the Information Commissioner (ICO). Everyone subject to this policy must assist with any such assessment, audit, investigation or action as required by the ICO and / or the council.

## 9.2. The Data Protection Officer (DPO)

The council is required to appoint a DPO. The DPO is currently the Chief Officer of Legal and Democratic. Their responsibility is in respect of personal data, collected, held and processed by the council. They will be involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The DPO's responsibilities include the following.

- Ensuring that
  - → the council complies with the data protection laws,
  - → the council and council staff are fully informed of their own legal responsibilities and training of staff, and
  - → necessary arrangements are in place for dealing where appropriate with subject access requests that relate to more than one service of the council.
- Developing and managing the council's Data Protection Policy, including development, implementation and enforcement of this policy and data protection procedures.
- Reporting on the council's compliance with the data protection laws to the SIRO on a six-monthly basis.
- Providing advice when requested as regards data protection impact assessments and monitor their performance;
- Co-operating with, acting as a point of contact for, and consulting with the ICO, as required.

## 9.3. The Chief Executive and Chief Officers

The Chief Executive and each Chief Officer's responsibilities include the following.

- Ensuring that
  - → the information under their control is collected, processed and held in accordance with this policy and the data protection laws,
  - → necessary arrangements, including nominated officers, are in place to deal with subject access requests,
  - → necessary arrangements are in place within their Service for the secure disposal of personal data, and
  - → all processing of personal information complies fully with all the provisions of the data protection laws and this policy.
- Nominating lead contacts for data protection responsibility within their Services to the DPO; and immediately reporting changes of contact details to the DPO.
- Identifying and documenting
  - → all categories of personal information held within their service,
  - → all processing applied to that personal information, and
  - → how long personal information needs to be held within each Service.
- Implementing
  - → procedures for the secure destruction of any personal information immediately when the council no longer needs to keep it,
  - → arrangements and procedures as necessary for the safekeeping and preservation of all personal information held by their Services and ensuring that no one can get unlawful access to personal information that is held, and

→ procedures and issuing instructions to make sure that every person who has access to personal information held by their Service makes use of that information only for the purposes for which that information is held.

### 9.4. Business managers

Business managers' responsibilities include:

- Ensuring that
  - → employees and workers know what they have to do under the data protection laws and are trained in data protection,
  - → confirming to the DPO when appropriate training has been undertaken by employees and maintaining records of training,
  - → disciplinary action up to the point of dismissal is taken where an employee or worker has deliberately breached the terms of the data protection laws or this policy or of any of the council's own procedures,
  - → employees and workers know that they could face criminal proceedings if they deliberately or recklessly destroy information, obtain information or disclose it unlawfully.
  - → personal information held is accurate and up to date.
- Determining whether a Data Privacy Impact Assessment (DPIA) needs to be undertaken and, if so, putting in place appropriate arrangements to ensure that such a DPIA is undertaken and completed.

### 9.5. All users

All users must:

- Observe and comply with the data protection principles.
- Ensure that
  - → personal information is properly protected at all times – this requires continued compliance with the data protection laws, this policy and all other council information policies, procedures and guidance, and
  - → individual archives, or any personal records they hold, are not kept when they are no longer required.
- Report any observed or suspected breach of this data protection policy or related information procedures and guidance.

## 10. Privacy by design and Data Privacy Impact Assessments (DPIAs)

We are required to implement **privacy by design** measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. Pseudonymisation describes removing or replacing information within data set which identifies an individual.

Users must assess what privacy by design measures can be implemented on all programs, systems and processes that process personal data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

The council must also conduct DPIAs in respect to high-risk processing.

Services should conduct a DPIA (and discuss the findings with the DPO) when implementing major system or business change programs involving the processing of personal data including:

→ use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

→ automated processing including profiling and automated decision making;

→ large scale processing of special categories of data; and

→ large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

1. a description of the processing, its purposes and the council's legitimate interests, if appropriate;
2. an assessment of the necessity and proportionality of the processing in relation to its purpose;
3. an assessment of the risk to individuals; and
4. the risk mitigation measures in place and demonstration of compliance.

The DPO is responsible for producing guidance on DPIAs and reviewing the guidance every alternate year commencing October 2012.

# 11. Data protection incidents and breaches

The UK GDPR requires data controllers to keep a written record of data breaches, near misses or incidents. This is kept by the council's DPO.

- Where any breach is assessed as resulting in a risk to the rights and freedoms of the individual(s) affected there is a requirement to notify the ICO of the breach within 72 hours of the breach occurring.
- Where the breach is likely to result in a high risk to the rights and freedoms of affected individuals the UK GDPR requires that the individual(s) is/are informed without undue delay.
- All incidents must be reported using the Data Breach form, whether or not the incident results in a breach of the data protection laws and/or actual damage or loss to any person, to the DPO in accordance with the Data Protection Breach and Incident Management Protocol. The DPO will take appropriate action in respect of the incident, in accordance with the said protocol. Incidents are defined/explained the protocol.

# 12. Data protection fee

It is the responsibility of the DPO to ensure payment of the annual data protection fee to the ICO and to provide all information required by the ICO when doing so.

# 13. Documenting data processing activities

The council must document and maintain a written record of its data processing activities.

The DPO is responsible for ensuring that all categories of personal information and data subjects held by the council are documented, including:

1. the uses to which the information is put;
2. the categories of recipients of the personal information;
3. details of transfers to third countries (including the transfer mechanism safeguards in place);
4. the period for which the information will be held; and
5. a description of the technical and organisational measures in place to keep the information secure.

To enable the documentation to be kept up to date at all times, it is the responsibility of the Chief Executive, the Depute Chief Executive and each Chief Officer to advise the DPO immediately of any:

- new categories of information or data subjects held in his/her service;
- changes in the uses to which his/her service is putting any personal information his/her service holds;
- categories of personal information or data subjects which are no longer held by his/her service;
- changes in categories of recipients of personal information held in his/her service;
- changes in the transfer of personal information to third countries (including the transfer mechanism safeguards) in his/her service;
- changes in the retention periods for personal information held in his/her service; and
- changes in the technical and organisational measures in place to keep information secure in his/her service.

# 14. Sharing information with other council services and third parties

The council must protect against processing personal information unlawfully. In most cases personal information can only be shared between council services and/or third parties where the individual concerned knows that such sharing may happen and where the processing complies with the data protection principles. The first data protection principle states that personal information shall be processed fairly, lawfully and in a transparent manner.

Personal data that is provided to a service within the council is not automatically available to all **other council services**.

- It is important to understand the purpose or purposes for which the information was originally obtained and whether the data subject would reasonably anticipate that this information would be shared with another council service.
- Personal information can be shared between council services where there is a lawful basis to do so, and data subjects are generally aware of how the data will be used.

Where a request for personal information is received from a **third party**, the identity of the requester and the need for the information must be known before consideration is given to providing it.

- Personal information can be given to the police or the procurator fiscal to help with a criminal investigation and to certain statutory authorities/agencies (such as DWP and HMRC).
- This only applies in certain circumstances, so such requests for disclosure must be made in writing, providing details of the data subject, reason for disclosure, name of requesting officer and certification by a senior officer.
- A record must be kept of all such disclosures by services and a report made available to the DPO immediately upon request.

In all cases, if there are any concerns at all about an enquirer or their enquiry, information must not be given out and the enquiry should be referred to the DPO.

# 15. Data sharing

Generally, the council is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

Services and officers might be approached and asked if the council will enter into **a data sharing agreement** with another organisation. A data sharing agreement addresses arrangements whereby one organisation shares personal data with another organisation.

The council will only share personal data it holds with third parties if:

1. they have a need to know the information for the purposes of providing the contracted services;
2. sharing the personal data complies with the Data Protection Principles;
3. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
4. the transfer complies with any applicable cross border transfer restrictions; and
5. any necessary information sharing or data processing agreements are in place.

A statutory Data Sharing Code of Practice in respect of data sharing arrangements between organisations has been issued by the ICO under Section 121 of the Data Protection Act 2018.

The code explains how the 2018 Act applies to the sharing of personal data. It provides practical advice to organisations that share personal data and covers systematic data sharing arrangements as well as ad hoc or one-off requests to share personal data.

Data sharing agreements should be approved by the business manager for the service concerned and the negotiation and adjustment of the necessary legal documentation should be referred to the DPO and the Chief Officer of Legal and Democratic services, who will hold the signed completed agreements. The council holds a record of all data sharing agreements.

# 16. Transferring personal information outwith the UK or EEA

The council will not transfer personal data outside the European Economic Area (EEA) unless this cannot be avoided.

1. The council will only transfer data outside the UK and the EEA when it is satisfied that the party which will handle the data and the country it is processing it in will provide adequate safeguards for personal privacy.
2. If the council need to transfer any personal information overseas in relation to a particular activity, this will be explained in the specific privacy statements relating to that function along with a description of the protective measures we have put in place to keep it secure.

# 17. Rights of individuals

All users must respect the rights of all individuals (data subjects), including employees and elected members. These include rights to:

- receive certain information about the council's processing activities;
- request access to their personal data that we hold;
- prevent our use of their personal data for direct marketing purposes;
- ask us to erase personal data
  - → if it is no longer necessary in relation to the purposes for which it was collected or processed,
  - → to rectify inaccurate data, or
  - → to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- object to decisions based solely on automated processing, including profiling;
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- where processing is based on consent, withdraw consent to processing at any time;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the ICO; and
- in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

The identity of an individual requesting data under any of the rights listed above should be verified before disclosing any personal information.

# 18. Product set

The table below lists documents in the Data Protection Policy product set and other related products. This may include links to other file types, websites and IT systems.

- Those listed under policies, procedures and guidance are the responsibility of the Data Protection team.
- Those listed under related products are the responsibility of other teams or services.

| Product type | Product |
|---|---|
| Procedures | ▪ Data Breach form<br>▪ Data Protection Breach and Incident Management Protocol<br>▪ Data Protection Impact Assessment Template<br>▪ Data protection procedures and guidance<br>▪ Register of Data Sharing Agreements |
| Guidance | ▪ DPIA and Lawful Bases<br>▪ SAR Guidance |
| Related products | ▪ Acceptable Use of IT Policy<br>▪ Digital and IT Strategy<br>▪ Discipline Policy<br>▪ Information Asset Register<br>▪ Information Security Policy<br>▪ Records and Information Management Policy<br>▪ Records Retention Schedule<br>▪ Risk Management Strategy<br>▪ Payment Card Data Security<br>▪ Privacy notice |
| Legislation, regulations, and government guidance | ▪ Councillors' Code of Conduct<br>▪ Data Protection Act 2018<br>  ▪ Schedule 1 of the Data Protection Act 2018<br>  ▪ Section 121 of the Data Protection Act 2018<br>▪ ICO guidance on the UK General Data Protection Regulation<br>  ▪ ICO Data Sharing Code of Practice<br>  ▪ ICO guidance to organisations on the UK GDPR<br>  ▪ ICO special category data<br>▪ The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020<br>▪ UK General Data Protection Regulation<br>  ▪ Article 9 of the UK GDPR<br>  ▪ Article 10 of the UK GDPR |

# Appendix 1: Glossary of terms

| Term | Description |
|---|---|
| **The Act** | Data Protection Act 2018 |
| **All users** | All parties who have access to council information including employees, elected members and third-party contractors and any other individuals or organisations who access council information. |
| **Council information** | Council information includes data, records, paper and digital formats. |
| **Controller** | The people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the data protection laws.<br>The council is the controller of all personal data used in its business. |
| **Data protection laws** | The UK GDPR and the Act |
| **DPO** | Data Protection Officer |
| **DWP** | Department of Work and Pensions |
| **The UK GDPR** | UK General Data Protection Regulation |
| **HMRC** | Her Majesty's Revenue & Customs |
| **ICO** | Office of the Information Commissioner |
| **Personal data** | Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **Processing** | Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |

| Term | Description |
| --- | --- |
| **Processor** | Any person who processes personal data on behalf of a controller such as the council.<br><br>Council employees are excluded from this definition but it could include suppliers which handle personal data on behalf of the council, for example where the council outsources IT, payroll, paper waste disposal, and mail shot / marketing services. |
| **SIRO** | Senior Information Risk Owner. |