



North Ayrshire Council

Comhairle Siorrachd Àir a Tuath

Data Protection Policy

Version: 2.5

Date: 16th December 2022

Version	Date Issued	Author	Update Information
V1.0	15.11.12	Hazel Lauder	Approved by Cabinet 23 October 2012
V2.0	25.08.15	Rose Johnston	Approved by Cabinet 18 August 2015
V2.1	30.06.16	Rose Johnston	Minor changes to contact information
V2.2	21.05.18	Rose Johnston	Amended to reflect legislative changes
V2.3	29.01.19	Rose Johnston	Amended to reflect legislative changes
V2.4	16.12.22	Lauren Lewis	Amended wording and minor changes to contact information
V2.5	10.01.22	Lauren Lewis	Minor changes (accessibility)

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available only on our website. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

Document Control Guidelines

Prepared By: Senior Manager/Data Protection Officer (Information Governance)

Original Authorisation By: Corporate Management Team

Reviewed By: L Lewis – Senior Manager, Information Governance

K Hamilton – Information Management Officer

L Taylor – Solicitor, Legal Services

Published Location: External Website and Council intranet

Other documents referenced

Contents Listing

1.	Introduction	3
2.	Policy Statement	4
3.	Data Protection Principles	5
3.1	Personal & Special Categories (Sensitive Personal) Data.....	5
3.2	Data Protection Principles	6
4	Notification of Processing Activities	7
4.1	Registration	7
4.2	Disclosure of Data	8
4.3	Information Asset Register	8
4.4	Data Subject Rights.....	8
5	Roles & Responsibilities	9
5.1	Employees.....	9
5.2	Data Protection Governance Arrangements.....	9
6	Information Sharing	10
6.1	Data Processors	10
7.	Data Protection Impact Assessment	10
8	Management of Data Incidents and Breaches	11
9	Review	11
	Appendix 1 - Definitions	12
	Appendix 2 – Information Sharing Checklist	Error! Bookmark not defined.

1. Introduction

North Ayrshire Council is required by law to comply with the Data Protection Act 2018 (DPA). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not unlawfully disclosed to any third party.

North Ayrshire Council regards the lawful and correct treatment of personal information vital to its successful operations, and to maintaining confidence between the Council and those with whom it carries out business. We want users of our services to feel confident about the privacy and security of their personal information.

The Council is committed to a policy of protecting the rights and privacy of individuals (this includes customers, staff and others) and fully endorses and adheres to the Data Protection Legislation.

[Appendix 1](#) of this document contains technical terms used in this document.

The DPA regulates the processing of information relating to **living** persons in the UK. It requires that data controllers be registered with the UK Information Commissioner and comply with the legally enforceable principles.

In order to operate, the Council needs to process certain information about members of the public; current, past and prospective employees, clients and customers; and business partners.

It may be required by law to collect and use information to comply with the legislative requirements. The safeguards within the DPA are to ensure that personal information is handled and dealt with properly.

If you require any further information or are unsure about any aspect of data protection you should contact the Council's [Data Protection Officer](#) for further guidance.

2. Policy Statement

This policy will be published on the Council's Intranet and external facing website. Amendments or revisions will be noted within the document control section. A review will be undertaken every two years. However, policies and guidelines may be altered at any time if amendments are necessary.

This policy applies to all Employees and Elected Members of the Council. Any breach of the Data Protection legislation or the Council's Data Protection Policy is a serious matter and could lead to disciplinary action or criminal proceedings in extreme cases.

Other agencies and individuals working with the Council, and who have access to personal information held by the Council are required to comply with this policy.

Services who deal with external agencies processing Council information are responsible for ensuring those agencies sign a contract agreeing to abide by this policy.

This policy applies to all situations where the Council processes (collect, store, use, share) personal data about living individuals. It includes information stored in any format including but not limited to: electronically, on paper, on CCTV, in photographs and on audio equipment.

All sharing of personal data with other organisations must be appropriately documented. A **Data Processing & Sharing Agreement** must be in place when personal or business sensitive information is being shared with a third party by the Council.

In addition to the Data Protection Policy there are other key Council policies, supporting information groups, codes and guidance which are in place to support good information handling and further details are documented in [Section 4 Roles and Responsibilities](#)

3. Data Protection Principles

The purpose of the DPA is to protect the rights and privacy of living individuals. This ensures that personal data is not processed without their knowledge. The legislation is underpinned by a core set of principles. Adherence with these principles will ensure compliance with the DPA. The principles are: -

- Principle 1** Personal data shall be processed lawfully, fairly and in a transparent manner.
- Principle 2** Personal data shall be collected for specified, explicit and legitimate purposes
- Principle 3** Personal data shall be adequate, relevant and not excessive.
- Principle 4** Personal data shall be accurate and, where necessary, kept up to date
- Principle 5** 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 those data are processed
- Principle 6** Personal data shall be processed in a manner that ensures appropriate security of the personal data

3.1 Personal & Special Category Data

3.1.1 Personal Data

Personal Data means any information relating to an identified or identifiable person. This includes identifiers such as:

- Name
- Identification number
- Location data including address
- Online identifiers including IP address/cookies

Information can become personal data if it can be combined to identify an individual. This can include combining the following factors:

- Physical
- Physiological
- Genetic
- Mental
- Economic
- Cultural
- Social

3.1.2 Special Category Data

Special category data is a subset of personal data and stricter conditions apply to the processing of this type of data. This includes:

- the racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- information relating to health of the data subject
- sex life/sexual orientation

- the commission or alleged commission of any criminal offence
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings
- Biometric or genetic information

3.2 Data Protection Principles

North Ayrshire Council processes data in relation to its employees, clients, customers and business partners. The Council undertakes to comply with the data protection principles, which are at the core of the DPA and regulate when and how personal data should be processed.

Further information about why the Council manages personal data can be located within our [Privacy Policy](#).

3.2.1 Principle 1 – Processed Fairly, Lawfully and Transparently

North Ayrshire Council will ensure that it has appropriate grounds for processing personal data and ensure it is not used in ways that could have unjustified adverse effects on the individuals. We will ensure that the processing matches the description given to the data subject and highlight any special category or criminal conviction data that will be processed and the relevant processing basis.

All sharing of personal data with other organisations will be appropriately documented.

3.2.2 Principle 2 – collected for specified, explicit and legitimate purposes

North Ayrshire Council must ensure that data is processed for limited purposes. Where personal data is collected, the data subject will be provided with a fair processing or privacy notice, providing information about what we collect, why this information is needed and how it will be processed. When processing special category data we will ensure that this is in accordance with and reflects the relevant processing conditions set out within the DPA.

3.2.3 Principle 3 – Adequate, Relevant and limited to what is necessary

North Ayrshire Council will identify and collect the minimum amount of information required for the purpose. If it becomes necessary to hold or obtain additional information about certain individuals, that information will only be collected and recorded in relation to those individuals. We will ensure that the use of special category or criminal conviction data is limited to that which is essential to the purpose of processing.

3.2.4 Principle 4 – Accurate and, where necessary, kept up to date

North Ayrshire Council will have processes in place to ensure that all relevant information is kept accurate and up to date. Where the Council identifies an inaccuracy or a data subject indicates that the information held by the Council or a business partner is inaccurate, the error will be rectified by the relevant Service in conjunction with the Data Protection Officer, where necessary.

3.2.5 Principle 5 – Kept no longer than is necessary for the purposes for which those data are processed

North Ayrshire Council will implement procedures in relation to the retention of personal data in accordance with the Corporate Records Retention Schedules and ensure that we comply with the provisions of the Public Records (Scotland) Act 2011.

The Council will - where it is possible - store personal data in a way that limits or prevents identification of the data subject and will in any event ensure that personal data is disposed of in accordance with our retention schedules.

Each Service has a responsibility to ensure that appropriate retention schedules are in place for the records that they hold and secure destruction methods are in place. This applies to both electronic and paper records.

3.2.6 Principle 6 –Personal data shall be processed in a manner that ensures appropriate security of the personal data with regard to technical and organisational measures

The Council must evidence and demonstrate to its customers, partners and stakeholders that it can be trusted to protect the confidentiality, integrity and accessibility of the information it holds.

All personal data will be appropriately safeguarded against accidental destruction, theft or any other loss. At all times we will ensure that the confidentiality and integrity of the personal data is maintained.

Where personal data has to be taken off-site this will be restricted to only that which is necessary to undertake the required task. Documented procedures will be in place to mitigate against any loss.

North Ayrshire Council has further guidance and policies available in terms of [ICT Security](#) which further addresses the requirements of this principle.

4 Notification of Processing Activities

4.1 Registration

The [Data Protection \(Charges and Information\) Regulations 2018](#) requires organisations that processes personal information to pay a fee to the Information Commissioner's Office (ICO), unless exempt. The ICO maintains a public register of notified data controllers. The Council is registered under entry number [Z4840237](#)

The Council has an [Information Asset Register](#) which forms the basis of the Council's documentation of processing activities.

It is the responsibility of the Services' Information Asset Owners to update the register and ensure entries are accurate at all times. The register will be managed by the Council's Information Governance Team.

When processing personal information as a member of the council, Elected Members are covered by the Council's notification and when acting on behalf of their political party they are entitled to rely on the party's notification.

When processing personal information on behalf of constituents, Elected Members are data controllers in their own right.

4.2 Disclosure of Data

The Council must ensure that personal data is not disclosed to unauthorised third parties. All employees and Elected Members must ensure there is a lawful basis to share personal data before disclosing to a third party. Personal data can be disclosed where one of the following legal bases apply:

- The individual has given their explicit consent
- Where the disclosure forms part of the Council's statutory task and where DPA permits such disclosure without consent in relation to specific purposes
- Where the Council is legally obliged to disclose data
- Where disclosure of data is required in relation to a contract which the individual has entered into
- If the sharing of information is necessary in the vital interests of the data subject

4.3 Information Asset Register

All proposed systems or systems under development which process personal data must be checked prior to final approval to ensure that the data processing will be covered by our [Privacy Policy](#).

All systems (paper & electronic) which process personal data will be recorded on a central database, the **Information Asset Register**.

4.4 Data Subject Rights

Data Subjects have rights under DPA regarding data processing, and the data that is recorded about them. These rights include

- Right to be informed
- Right of access
- Right to rectification of inaccurate data
- Right to erasure in certain circumstances
- Right to object to certain processing, including the right to prevent processing for direct marketing
- Right to prevent automated decision-making and/or profiling
- Right to data portability
- Right to claim compensation for damages caused by a breach of data protection

An individual has the right to access his/her own personal data. The Council has **one month** to comply with a request for Subject Access Request (SAR).

No fee will be charged unless the Data Protection Officer considers the request to be manifestly unfounded or excessive and in these cases shall determine the appropriate level of charge.

Further information on compliance with all data subject rights by contacting the [Information Governance Team](#).

5 Roles & Responsibilities

In recognition of our data protection obligations and in addition to this policy a range of policies, procedures and guidelines promoting compliance and best practice have been developed to support a robust data governance framework.

- [Acceptable Use Policy](#)
- [Data Breach Reporting and Management Procedures](#)
- [Records Management](#)
- [Data Protection Impact Assessment Framework](#)
- [Freedom of Information](#)
- [Information Asset Register](#)
- [Subject Access Requests](#)
- [Privacy Notice](#)
- [Redaction Guidelines](#)

The list is not exhaustive and all relevant data protection and wider information management guidance can be located under the Information Governance section on the Council intranet.

5.1 Employees

All employees and Elected Members are individually responsible for ensuring that processing of personal data is in accordance with the DPA and this policy. It is the responsibility of the individual to familiarise themselves and comply with Council policy and guidance.

Advice can be sought from the Data Protection Officer or the Information Governance Team who have responsibility for ensuring corporate compliance with the data protection legislation.

5.2 Data Protection Governance Arrangements

As a controller of data the Council has a corporate responsibility to demonstrate its commitment to data protection and to effectively evidence compliance. Under the DPA, the Council must appoint a Data Protection Officer whose key tasks are to;

- Inform and advise the Council of data protection compliance
- Monitor Compliance
- Provide advice and provide corporate sign off for Data Protection Impact Assessments (DPIA)
- Train employees in data protection
- Conduct information audits
- Be the first point of contact for the regulator (Information Commissioner's Office)
- Have regard to the risk associated with the Council's processing activities

The [Data Protection Officer](#) (DPO) has the corporate responsibility to develop, implement and communicate the Council's Data Protection Policy and procedures.

The Council's [ICT & Cyber Security Architect](#) ensures compliance with principle six of the DPA relating to data security by providing advice and guidance on information security.

The [Information Management Officer](#) will promote good information management through the provision of advice and guidance to services and has responsibility for information and records management.

6 Information Sharing

Processing of personal and special category data must always be fair, lawful and transparent. The DPA provides a framework to ensure that when personal information is shared that it is:

- appropriate
- proportionate
- on a need-to-know basis

Refer to the Council's intranet for further guidance on Information Sharing.

There are many situations where information can, and legally, must be shared. In these circumstances of information sharing the following must be considered:

- What information needs to be shared?
- With Whom?
- Why?
- How?
- What are the risks of not sharing the information?
- Could the same aim be achieved without sharing the data or by anonymising it?

6.1 Data Processors

Where a third-party processes information on behalf of the Council, the Council is known as a **Data Controller** and the third party is the **Data Processor**. There must be a written agreement in place to evidence the data relationship. This is known as a data sharing and processing agreement and documents the handling controls in place.

The Council publishes its [Information Governance Procurement Framework](#) on the Council intranet. The purpose of this is to help those involved in supply chain activities to assist, with regard to data protection management, in the:

- Identification of information governance requirements
- Mitigation of information risk within the procurement process

7. Data Protection Impact Assessment

Data Protection Impact Assessments (DPIA) replaces Privacy Impact Assessments (PIAs) and in certain circumstances are mandatory to carry out prior to processing personal data.

DPIA is a process which enables the Council to address the potential privacy risk and impact from collecting, using and disclosing of personal information as part of proposed new initiatives. A DPIA will ensure data protection compliance and privacy concerns are appropriately addressed.

Services must also undertake a DPIA before making major changes to an existing way of handling information.

The purpose of a DPIA is to;

- identify any potential and likely impact on privacy;
- minimise and manage any identified impact and privacy risk;
- ensure a “privacy by design” approach;
- demonstrate compliance with data protection legislation.

Guidance and details on how to conduct a [Data Privacy Impact Assessment](#) can be found on Council intranet. Advice on and assistance with carrying out a DPIA can be obtained from the Data Protection Officer.

In cases where the processing risks are high and cannot be reduced you should consult with the DPO if you still intend to process the data as it may be necessary to inform the Information Commissioner’s Office (ICO) of the intention to process in these circumstances. Contact with the ICO must only be carried out by the Data Protection Officer as part of their legislative duty.

8 Management of Data Incidents and Breaches

The Council has a legal responsibility to ensure that personally identifiable information about individuals is processed securely, held confidentially and with integrity and accessed only by those who have a justified right of access. In the event of this principle being breached, the Data Protection Officer must be notified immediately. This will allow for an investigation to be undertaken and for the DPO to assess whether reporting to the ICO is required. The legislative timescale to report to the ICO is 72 hours from becoming aware of the breach. Failing to report an incident or doing so late may result in regulatory action being taken by the Commissioner.

Further information on how to report a data breach can be found in the [Data Breach Reporting and Management Procedures](#).

Breach of this policy may be regarded as a serious act of misconduct and may lead to disciplinary action. Employees must therefore make every effort to ensure that they understand their responsibilities under this policy.

It is a criminal offence under the DPA to knowingly or recklessly obtain, disclose or procure personal data without the consent of the Data Controller and North Ayrshire Council reserves the right to report any such incidents to the Information Commissioner’s Office and/or Police Scotland.

9 Review

This policy will be reviewed on a two-yearly basis, unless earlier review is deemed necessary by changes in legislation, regulatory guidance, or a change in Council policy.

Appendix 1 - Definitions

Data Controller: Any person (or an organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Processor: Any person (or organisation) contracted by a data controller to process information on their behalf. The data controller retains legal liability for the processing and protection of the information.

Data Processing and Sharing Agreement: Ensures the "rules" of sharing have been clearly communicated and understood by all parties. Aims to ensure that methods of sharing, storing, use, in transit, backups, destruction, etc. are agreed before sharing is undertaken.

Data Subject: Any living individual who is the subject of personal or sensitive data.

Information Asset Owner: The business manager who operationally runs and is responsible for the information asset; their role is to understand what information is held and how it is processed.

Information Asset Register Central log located on Council intranet which records all systems (paper & electronic).

Information Commissioner Office (ICO) : The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Information Sharing Protocol : Is a commitment and agreement to put in place the arrangements required to ensure secure and appropriate sharing of information and data between organisation, whilst maintaining the controls that give assurances and accountability and respects the right to privacy.

Personal Data: Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, national insurance number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Processing: Any operation related to the holding, organisation, retrieval, disclosure and deletion of data and includes obtaining and recording data; accessing, altering, adding to, merging, deleting data; retrieval, consultation or use of data; disclosure or otherwise making available of data.

Special Category Data (Sensitive) Personal Data: Different from personal data, relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life or criminal convictions, biometric, genetic. This type of data is subject to much stricter conditions of processing.

Third Party: Any individual/organisation other than the data subject, the data controller or its agents.