Data Protection Policy

August 2025

Version 2.0

Version control template

Date of Creation:	July 2025
Owner (Service):	Information Governance Manager & DPO
Reviewer Head of Service:	Head of Governance, Strategy & Performance
Approver Executive Director:	Depute Chief Executive (Education, Communities and Organisational Development)
Date Approved:	
Approver (Committee):	Corporate Committee
Date Approved:	26th August 2025
Next Review Date:	

Version History

Version	Date	Author	Changes Made	Approved By
1.0	May 2018	Records & Heritage Manager	Initial document	Corp Ctee
2.0	Aug 2025	Information Governance Manager & DPO	GDPR updated to UK GRPR. AI section added. Privacy Notice webpage link added.	Corp Ctee

Contents

Definitions 3

1. Data Protection Policy Statement 5
2. Introduction 6
3. The Data Protection Principles 6
4. Lawful Bases for Processing Personal Information 7

Personal Data Lawful (Legal) Bases 7

a) Consent: 7
b) Contract: 7
c) Legal obligation: 7
d) Vital interests: 7
e) Public interest: 7
f) Legitimate interests: 7

Special Category Data & Criminal Offence Data 8

5. Data Subject Rights 8
6. Information Commissioner's Office (ICO) 9

Registration and Fees 9

7. Roles and Responsibilities 9

Senior Information Risk Owner 9

Information Asset Owners 9
Data Protection Officer (DPO) 9
Information Security Officer 10
Information Assurance Group (IAG) 10
Employees 10
Elected Members 11
8. Processing Personal Data 11
Data Sharing/Processing Agreements 11
Privacy Notices 11
9. Personal Data Breaches 12
10. Training 12
11. Artificial Intelligence (AI) 12
12. Further Information and Legislation 12

Definitions

Accountability Principle: This requires the Council to be responsible for its own compliance with Data Protection Legislation and to demonstrate that compliance.

Controller: A person, usually an organisation, which alone, or jointly with others, determines the purposes for and manner in which personal data is used (how and why to process personal data). This includes employees of the controller. The Council is considered to be the controller for most of its activities that involve personal data.

Criminal Offence data: The UK GDPR gives extra protection to "personal data relating to criminal convictions and offences or related security measures". The Information Commissioner's Office (ICO) refer to this as 'criminal offence data' and clarify that this covers a wide range of information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings. It includes not just data which is obviously about a specific criminal conviction or trial but may also include personal data about unproven allegations and information relating to the absence of convictions. It also covers a wide range of related security measures, including personal data about penalties, conditions or restrictions placed on an individual as part of the criminal justice process, or civil measures which may lead to a criminal penalty if not adhered to. It does not cover information about other individuals, including victims and witnesses of crime.

Data Protection by Design and by Default: an integral element of accountability. It necessitates embedding data protection into everything the Council does, throughout all processing operations, while documenting the decisions the Council takes (for example in Data Protection Impact Assessments (DPIAs)). Measures that the UK GDPR suggests as potentially appropriate includes minimising the data collected, applying pseudonymisation techniques, and improving security features.

DPA 2018: the Data Protection Act (DPA) 2018, which sits alongside the UK GDPR and sets out the framework for data protection in the UK.

Data Protection Legislation: means any law applicable to the processing, privacy and use of personal data, including the DPA 2018, the UK GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). It also includes any amendments, or successor legislation.

Data Subject: An identified or identifiable living individual to whom personal data relates.

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. It also includes any expression of opinion about the individual and any indication of the intentions of the controller or any other person in respect of the individual – e.g., a manager's assessment of an employee's performance during their probation period.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Processor: A person (usually an organisation) that processes data on behalf of and as specified by the controller. This will always be a third-party with whom the controller has a contract that specifies what, how and the other conditions under which the data will be processed.

Record of Processing Activities (ROPA): A requirement under UK GDPR Article 30 and part of accountability; this is a record that the Council must maintain of its processing activities, including the purposes for the processing, any data sharing and retention.

Special Category Data: This is personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data (where used for ID purposes), data concerning health or data concerning a data subject's sex life or sexual orientation. Special category personal data is subject to much stricter conditions of processing. Personal data relating to criminal convictions and offences are not included but similar extra safeguards apply to its processing.

Processing: Means any operation or set of operations performed on personal data. This includes collecting, storing, recording, using, amending, analysing, disclosing or deleting it.

Third party: Anyone other than the data subject, controller, processor and others who, under the direct authority of the controller or processor, are authorised to process personal data.

UK GDPR: the UK version of the European Union General Data Protection Regulation (GDPR), as amended and incorporated into UK law by the European Union (Withdrawal) Act 2018, and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

1. Data Protection Policy Statement

In order to carry out many of its functions and responsibilities, Moray Council (the Council) must process personal data. The individuals whose data is processed, such as by collecting, storing, sharing and suchlike, may include members of the public, current, past and prospective employees, customers and service users, and, suppliers.

This Policy sets out the Council's commitment to ensuring that all personal data processed by the Council is managed appropriately, in accordance with Data Protection Legislation (including the Data Protection Act 2018 (DPA 2018) and the United Kingdom General Data Protection Regulation (UK GDPR)). This commitment is imperative for compliance with the Council's legal obligations, and, to contribute to the maintenance of confidence between the Council, its customers and service users, employees and those with whom it carries out business.

Personal data in all formats are covered by this Policy. This includes, but is not limited to:

- hardcopy information such as paper files,
- electronic information, such as in databases, emails, and,
- media, such as audio recordings (i.e. telephone recordings and voicemails) and images (i.e. CCTV footage, photographs).

The Council recognises that a personal data breach if not addressed in an appropriate and timely manner, can result in physical, material or non-material damage. Where personal data breaches do occur the Council will, without undue delay, seek to contain the harm to individuals, investigate the breach, and where appropriate report the breach to the ICO, as well as to learn the lessons from any actual or suspected breaches.

This Policy applies to all employees and elected members as well as consultants, volunteers, contractors, agents or any other individual(s) performing a function on behalf of the Council. It seeks to assist all such individuals with Data Protection compliance and embed a Data Protection compliance culture within the Council. Violations of this Policy may result in disciplinary action.

2. Introduction

Data Protection legislation provides a framework that ensures personal data is properly managed and gives individuals rights to know how personal data may be processed, including how it is collected, used and stored.

Data Protection legislation dictates:

- The Data Protection Principles,
- The lawful bases under which Personal Data may be processed,
- Data Subject Rights, including the right to erasure, right of access (i.e. Subject Access Requests), and, sets timescales for compliance with these rights,
- How personal data should be processed; including transparency, i.e. Privacy Notices
- The requirements for recording and responding to personal data breaches, and,
- The requirement for an organisation's ICO registration, and, appointment of a Data Protection Officer (DPO)

3. The Data Protection Principles

UK GDPR sets out seven key legally enforceable principles that lie at the heart of the UK data protection regime. Under UK GDPR Article 5, personal data shall be:

i. processed lawfully, fairly and in a transparent manner in relation to data subjects (**'lawfulness, fairness and transparency'**)

ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that's 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 (**'purpose limitation'**)

iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)

iv. 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 (**'accuracy'**)

v. 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 UK GDPR in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**)

vi. 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 (**'integrity and confidentiality'**).

And,

vii. The seventh principle is **accountability**; this requires the Council to be responsible for its own compliance with Data Protection Legislation and to demonstrate that compliance.

Under UK GDPR Article 24(1), the Council must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR; the measures should be risk-based and proportionate; and reviewed and updated as necessary.

The UK GDPR sets out several different measures organisations can take to meet accountability obligations, these include:

- Implementing data protection policies,
- adopting a data protection by **design and default** approach,
- ensuring contracts are in place (also known as a data processing agreement) with all processors that handle personal data on its behalf, and,
- maintaining a ROPA.

The Council must also ensure that it maintains records of consent and of any personal data breaches.

As part of its accountability obligations, the Council also maintains an Information Asset Register (IAR), a register of Data Protection Impact Assessments (DPIAs), and a Data Sharing/Processing Register.

Compliance with these principles is key to data protection compliance. Failure to comply could lead to regulatory action by the Information Commissioner's Office (ICO); Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines and leave the Council open to substantial fines of up to £17.5 million.

4. Lawful Bases for Processing Personal Information

Personal Data Lawful (Legal) Bases

The lawful bases for processing are set out in UK GDPR Article 6(1). **Before** processing commences the lawful basis must be determined and documented, including within the Privacy Notice for the process. At least one of the below lawful bases must apply whenever the Council processes personal data:

a) **Consent:** the individual has given clear consent for the Council to process their personal data for a specific purpose.
b) **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.
c) **Legal obligation:** the processing is necessary for the Council to comply with the law (not including contractual obligations).
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public interest:** the processing is necessary for the Council to perform a task in the public interest or for the Council's official functions, and the task or function has a clear basis in law.
f) **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.

Special Category Data & Criminal Offence Data

UK GDPR gives extra protection to special category data and data about criminal convictions, criminal offences or related security measures. These types of data are subject to much stricter conditions of processing.

When the Council is processing special category data, or criminal offence data, an additional condition for the processing must be identified. For special category data, a condition under UK GDPR Article 9 must be identified. For processing criminal offence data, the Council also requires either 'official authority' or a separate condition for processing the data in compliance with UK GDPR Article 10. In both instances the Article 6 lawful basis for processing, and, the Article 9 special category data and/or Article 10 criminal offence data should be documented in Data Protection Impact Assessments (DPIA) so that the Council can demonstrate compliance and accountability.

Under the DPA 2018, the Council is required to have an Appropriate Policy Document (APD) in place when relying on certain specified conditions to process special category data and criminal offence data, which:

(a) explains the controller's procedures for securing compliance with the principles in Article 5 of the UK GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained.[1]

5. Data Subject Rights

Data Protection legislation provides data subjects with the following rights regarding their personal data:

- The right to be informed; including about how personal data will be used.
- The right of access to their personal data (Subject Access Request).
- The right to rectification; the right to require the Council to correct any inaccuracies.
- The right to request the erasure of any personal data held by the Council where the Council no longer has a basis to hold the data.
- The right to request that the processing of their personal data is restricted.
- The right to data portability (rarely applicable for Council processing)
- The right to object to the Council processing their personal data.
- Rights in relation to automated decision making and profiling.

Each of these rights has a common set of standards that the Council must adhere to; including that requests must be responded to within one calendar month.

[1] Schedule 1, Part 4, Paragraph 39 of the DPA 2018.

6. Information Commissioner's Office (ICO)

The ICO is the UK regulator for data protection and information rights; enforcing the Data Protection Act 2018, UK GDPR, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and more. There are a number of tools at the ICO's disposal to take action for a breach of Data Protection. These include: assessment notices, reprimands, warnings, enforcement notices and penalty notices (administrative fines). For serious breaches of the Data Protection principles, they have the power to issue fines of up to £17.5 million, or 4% of annual turnover, whichever is higher. Criminal prosecutions can also be pursued.[2] The ICO can also undertake an audit with an organisation to assess its compliance with Data Protection Legislation.

Registration and Fees

The Council, including the Licensing Board, are registered with the ICO; registration number **Z7512703**.

Elected Members, as Data Controllers, are exempt from paying the registration fee and are not required to be registered.

7. Roles and Responsibilities

Senior Information Risk Owner

The Council's Chief Executive is the Council's Senior Information Risk Owner (SIRO) in relation to Information Governance, which includes Data Protection.

Information Asset Owners

Information Asset Owners (IAOs) are the Council's Corporate Leadership Team and Heads of Service. The IAO's role is to understand what information is held by their departments and services, how it should be managed and ensure it is compliant. They must ensure that written procedures are in place and followed relating to these activities, risks are assessed and mitigated, and, the risk assessment processes are audited. The IAOs are also responsible for ensuring their department or service's IAR and ROPA entries are accurate and up to date.

Overall responsibility and accountability for ensuring that all staff and associated third parties comply with information legislation, this Policy and associated policies, procedures and guidance lies with the Senior Management Team.

Data Protection Officer (DPO)

The role of the Data Protection Officer is to:

- Inform and advise the Council and its employees about their obligations to comply with Data Protection Legislation,
- Monitor compliance with Data Protection legislation, including the assignment of responsibilities, awareness raising and training of staff,
- Provide advice and guidance about Data Protection, including advice regarding DPIAs and acts as a contact point for individuals (staff and customers) exercising their Data Subject Rights,

[2] For example, under s170 of the DPA 2018, it is a criminal offence for a person knowingly or recklessly-
(a)to obtain or disclose personal data without the consent of the controller,
(b)to procure the disclosure of personal data to another person without the consent of the controller, or,
(c)after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

- Ensure appropriate arrangements are in place between the Council and other organisations processing or sharing personal data,
- Manage, report and notify of any data protection breaches (data breaches),
- Co-operate with the ICO and act as their point of contact on issues related to the processing of personal data.

The Council's DPO is the Information Governance Manager, who can be contacted via dataprotection@moray.gov.uk

Information Security Officer

The Information Security Officer is responsible for creating, implementing and maintaining the Council's security policy and procedures to reflect changing local and national requirements. This includes requirements arising from legislation, security standards and national guidance.

The Information Security Officer will support service areas on achieving best practice and compliance with security requirements. The Council's Information Security Officer is the ICT Team Leader (Cyber Resilience and Information Security).

Information Assurance Group (IAG)

The purpose of the IAG is to co-ordinate the Council's information assurance activity by bringing together those with specific responsibility in this area. It provides strategic overview and co-ordination of Data Protection, Information Governance and Information Security issues within the Council including:

- Policies, guidance and working practices
- Development of good practice recommendations
- General advice and guidance
- Review of data breaches, producing learning actions where appropriate
- Communication and training
- Management of information risks
- Information retention and storage

Employees

All employees, elected members, and any other individuals with authorised access to the Council's information must be familiar with the requirements of Data Protection legislation. All have a responsibility to ensure that personal data is properly managed and protected at all times. This requires continued compliance with the Council's policies, procedures and other guidance.

If an employee is found to have breached this policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

It is the responsibility of all to promptly report any identified or reasonably suspected personal data breaches to line managers and the DPO as per the Guidance on Data Breach Management. The legislation makes it compulsory for organisations to report a personal data breach, which is likely to result in a risk to an individual's rights and freedoms, to the ICO within 72 hours of becoming aware. The 72-hour reporting deadline commences from the moment a Council staff member becomes aware of a breach. The DPO will investigate, decide whether a breach should be reported to the ICO and will handle the submission of relevant details.

Elected Members

Elected members, when acting as a member of the Council, such as as a member of a committee, they must abide by the requirement of employees stated above.

Elected members, when acting in their capacity as a representative of constituents of their ward, are Data Controllers in their own right. In this scenario they are responsible for processing personal data correctly and ensuring their own Data Protection compliance.

When an Elected Member is performing their Councillor duties they have a right to access Council information when it is reasonably required. When Elected Members are acting on behalf of a member of the public an Elected Member may need the written consent, normally by way of a mandate, from that individual.

8. Processing Personal Data

The Council will process personal data to support the wide ranging activities the Council carries out.

Data Sharing/Processing Agreements

When the Council shares personal data with other organisations the Council will comply with the provisions of the ICO's Data Sharing Code of Practice. It is good practice for the Council to have a written Data Sharing Agreement (DSA) in place when sharing personal data with another Controller on a routine basis. Having a DSA in place, ensures all parties understand the purpose of the sharing, what will happen at each stage and their various responsibilities. DSAs assist the Council in demonstrating compliance with its accountability obligations under Data Protection legislation.

This is separate from when the organisation is Processing Personal Data on the Council's behalf. Under UK GDPR, a Data Processing Agreement (DPA) or similar contract must be in place every time a Controller uses a Processor to process personal data; binding the Processor to the Controller in respect of its processing activities. Each DPA must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and, the Controller's obligations and rights.

The Information Governance team will review and advise on all such agreements prior to signature, then centrally register and store all such agreements. The final responsibility for signing and returning agreements lays with services. The Information Governance team will also highlight any other Data Protection requirements, such as DPIAs and Privacy Notices.

Privacy Notices

Under Articles 13 and 14 of UK GDPR, individuals have the right to be informed about the collection and use of their data. A privacy notice informs individuals what the Council does with their personal data including why the Council needs it, the legal basis for the processing and who the Council will share it with. Privacy notices must be provided to the prospective data subjects at the time their data is about to be collected.

The Council's Information Governance team hold the master copies of all Privacy Notices and maintains the publicly accessible webpage: www.moray.gov.uk/PrivacyNotices. Privacy Notices can be made available in other formats upon request.

9. Personal Data Breaches

The Council recognises that a personal data breach if not addressed in an appropriate and timely manner, can result in detriment to both the Council and the affected data subjects. Where personal data breaches do occur the Council will, without undue delay, put in place mitigations to contain any harm caused, investigate the breach, and where appropriate report the breach to the ICO. Lessons learnt from any actual or suspected breaches can then be reviewed with further mitigations implemented to reduce the likelihood of similar breaches in the future. A central register of personal data breaches is held by the Information Governance Team, and regular reports of breaches will be shared with Heads of Service and the IAG.

10. Training

All employees will be provided with Data Protection training as soon as reasonably practicable after starting to work for the Council. This essential training is available through CLIVE (LearnPro) as an online module, as well as a Data Protection Refresher module. Heads of Service are responsible for ensuring that employees within their Service are trained appropriately. Service specific Data Protection training can be organised with the Information Governance Team and is already available for Social Work via the Social Work Training Team.

Elected Members will also be provided with Data Protection training, initially as soon as reasonably practicable after they are elected.

Training should be renewed annually and must be refreshed when instructed to do so.

11. Artificial Intelligence (AI)

The Council is enthusiastic about the innovative and efficient opportunities presented by the rise of AI technology. The Council recognises that AI, if used effectively, has the potential to increase efficiency and innovation within the Council. However, AI technology also raises significant risks for the rights and freedoms of data subjects. As such, personal data should not be disclosed whilst using AI technologies until a DPIA has been completed and fully approved by the Council's DPO.

Whilst working, especially when working remotely, employees should be mindful of any 'smart products' such as virtual assistant technology; ensuring that these are not privy to work conversations or meetings, in which confidential or personal data is discussed.

12. Further Information and Legislation

- Data Protection Act 2018
- UK GDPR
- Information Commissioner's Office (ICO)

- Council Information Management Webpages:
  Includes: Data Protection, Records Management Plan, Re-Use of Public Information, Access to Information (including Freedom of Information)
- Interchange Information Governance Pages:
  Includes: Data Protection Guide, Guidance on Data Breach Management, Computer Use Policy, Corporate Information Security Policy