Data Protection Policy

Information Assurance Group

June 2018

Version 1.0

Based on the Information Commissioner's Office (ICO) Guidance on the Data Protection Act 2018 and General Data Protection Regulation (GDPR)

Document Control Sheet

Name of Document:	Data Protection Policy
Author	Records and Heritage Manager
Consultees	Information Assurance Group: including: • ICT Security Officer • Principal Librarian • Senior Solicitor • Internal Audit Manager • Acting Corporate Director (Education & Social Care) GDPR Project Officer Information Services Librarian
Description of Content	Data Protection Policy statement, and brief guide on the updated Data Protection Act 2018 and the General Data Protection Regulation (GDPR), both came into force May 2018.
Distribution:	Council wide upon approval
Status	Version 1.0
Date	25th May 2018

Contents

Definitions 3

1. Data Protection Policy Statement 4
2. Introduction 5
3. The Data Protection Principles 5
4. Lawful Bases for Processing Personal Information 6
5. Rights of Individuals 6
6. Information Commissioner's Office (ICO) 7
7. Roles and Responsibilities 7

Information Asset Owners 7

Data Protection Officer 7

Information Security Officer 7

Information Assurance Group 8

Employees and Elected Members 8

8. Processing Personal Information 8
9. Training 8
10. Further Information and Contacts 9

Links to Related Policies and Procedures 9

Definitions

Data controller: A body that determines the purposes for and manner in which personal data is used. This includes employees of the data controller. The Council is considered to be the data controller for most of its activities that involve personal data.

Data processor: A body that processes data on behalf of and as specified by the data controller. This will always be a third-party with whom the data controller has a contract that specifies what, how and the other conditions under which the data will be processed.

Data subject: A living individual to whom personal data relates.

Joint Data Controllers: These are people or organisations (for example, Moray Council, NHS Grampian or Police Scotland) who jointly process and share information.

Personal data: Any information relating to a data subject, particularly information that can be used to identify them 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 data 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 transmitted, stored or otherwise processed.

Special Category Data (also referred to as **Sensitive Personal Data**): This is personal data consisting of information as to any of the following:

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

Special category personal data is subject to much stricter conditions of processing. Personal data relating to criminal convictions and offences are not included but similar extra safeguards apply to its processing.

Processing: The definition of processing covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.

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

1. Data Protection Policy Statement

In order to operate efficiently Moray Council must collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, service users, and, suppliers. In addition, we may be required by law to collect and use information to comply with the requirements of government.

Moray Council will strive for a positive and proactive approach to data collection and management. The Council will ensuring we protect the information we collect; use and share information appropriately; actively managing it so it is relevant and up-to-date, and remain fully compliant with legislation and best practice guidance from the Information Commissioner's Office (ICO). Personal information in all formats are covered by this Policy, including but not limited to: paper files, databases, emails, telephone recordings, CCTV and all information repositories.

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 to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned. 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 Data Protection Policy applies to all employees and elected members as well as consultants, volunteers, contractors, agents or any other individual performing a function on behalf of the Council. Violations of this Policy may result in disciplinary action against an employee.

2. Introduction

Data Protection legislation, including the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR), provides a frameworks that ensure information is handled properly and gives individuals rights to know how personal information can be collected, used and stored.

There are some key differences between the previous Data Protection Act 1998 and the new legislation; the new rules which have been brought in mean:

- enhanced rights for individuals, such as right to erasure
- new documenting procedures – increased transparency about what we do with personal information; i.e. Privacy Statements
- ensure the minimum amount of information required is requested
- strengthening our rules for deleting and removing data
- notifying the Information Commissioner's Office (ICO) of certain breaches within 72 hours (and increased fines apply)
- dealing with Subject Access Requests within one calendar month
- appointing a Data Protection Officer (DPO) with responsibility for compliance

3. The Data Protection Principles

Data Protection Legislation sets out six principles for the processing of personal information that are legally binding on the Council. The personal information must be:

1. Processed lawfully, fairly and in a transparent manner in relation to data subjects
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by Data Protection Legislation in order to safeguard the rights and freedoms of the data subject.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Lawful Bases for Processing Personal Information

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

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

5. Rights of Individuals

Data Protection Legislation provides individuals with the following rights regarding their personal information:

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

For more information on Personal Data Rights please see:
Moray Council Website: Data Protection, and, A Guide to Personal Data Rights.
These will explain in more detail how to exercise your rights, including how to submit a Subject Access Request (SAR), and when a right does not apply.

6. Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

There are a number of tools available to the ICO for regulating the behaviour of organisations and individuals that collect, use and keep personal information. These include criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve a monetary penalty notice on a data controller.

The Council is registered with the ICO; registration number Z7512703.

7. Roles and Responsibilities

Information Asset Owners

The Information Asset Owners (IAOs) are the members of the Corporate Management Team. Their role is to understand what information is held by their services, what is added and what is removed, how information is moved, and who has access and why. Through their Heads of Service and management teams they must ensure that written procedures are in place and followed relating to these activities, risks are assessed, mitigated and the risk assessment processes are audited.

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

Data Protection Officer

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

- Inform and advise the Council and its employees about their obligations to comply with Data Protection Legislation, including DPA and GDPR.
- Monitor compliance of Data Protection, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations and related audits.
- Provide advice about data protection impact assessments (DPIAs) and monitor their performance;
- Co-operate with the supervisory authority (the ICO) and act as the contact point on issues related to the processing of personal data.

The Council's DPO is the Records and Heritage Manager, records@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.

Information Assurance Group

The Council's Information Assurance Group (IAG), among its various functions in relation to information management, assists the Council to implement the Policy. The IAG consists of: the DPO (Records & Heritage Manager), Senior Solicitor, ICT Security Officer, Internal Audit Manager and Principal Librarian.

Employees and Elected Members

All employees, elected members, and any other individuals with access to the Council's information must be familiar with the requirements of the Data Protection Legislation and have a responsibility to ensure that personal information is properly protected at all times. This requires continued compliance with the Council's information 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 employees to promptly report any identified or reasonably suspect data breaches to line managers and the DPO as per the Guidance on Data Security Breach Management. The GDPR 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 DPO will investigate, decide whether a breach should be reported to the ICO and will handle the submission of all relevant details.

8. Processing Personal Information

The Council will hold and process personal information only to support those activities it is legally entitled to carry out.

The Council may on occasion share personal information with other organisations. In doing so, the Council will comply with the provisions of the ICO's Data Sharing Code of Practice.

The person the personal information is collected from must be advised of the purpose for which the information will be held or processed and who the information may be shared with.

9. Training

All employees will be provided with training in basic data protection law and practice as soon as reasonably practicable after starting to work for the Council. This is available through CLIVE as an online module and is mandatory to all staff. Heads of Service are responsible for ensuring that employees within their Service are trained appropriately. Specific DPA training can be organised, and is already available for Social Work via the Social Work Training Team.

Elected Members will be provided with training in basic data protection as soon as reasonably practicable after they are elected.

Training should be renewed annually.

10. Further Information and Contacts

Further information is also available from the ICO's website or contact:

Information Co-ordinator,
Elgin Library
Cooper Park
Elgin
IV30 1HS
info@moray.gov.uk
01343562644

Links to Related Policies and Procedures

- Moray Council Information Management Website;
  Records Management Plan, Re-Use of Public Information, Freedom of Information, and, Data Protection general and Subject Access Request information

- Records Management Intranet;
  Records Management policies, Records Retention Schedule etc.

- Information Security Intranet;
  including Information Security Policy, Computer Use Policy.

- Complaints Handling Procedure

- Data Protection Act 2018

- General Data Protection Regulations (EU) 2016/679