APPENDIX A

Moray Integration Joint Board Records Management Plan

November 2018

Version 1.0

Document Control Sheet

Name of Document:	Moray Integration Joint Board; Records Management Plan
Author	Alison Morris, Records and Heritage Manager
Consultees	Moray IJB Board: Pam Gowans Margaret Forrest Information Assurance Group: including; Sean Hoath, Senior Solicitor; Mike Alexander, ICT Security Officer; Atholl Scott, Internal Audit Manager; Sheila Campbell, Principal Librarian Roddy Huggan, Commissioning Manager (H&SCM)
Description of Content	Information and links that address the 14 elements required to complete a Records Management Plan
Distribution:	Upon approval: Moray IJB wide, publically published and held by NRS
Status	Version 1.0. Accepted by Moray Integration Joint Board 29th November 2018
Date	November 2018

Contents

RECORDS MANAGEMENT PLAN

Summary

Moray Integration Joint Board (the Board) is fully committed to compliance with the requirements of the Public Records (Scotland) Act, which came into force on the 1st January 2013. MIJB will therefore follow procedures that aim to ensure that all of its officers, employees of constituent authorities supporting its work, contractors, agents, consultants and other trusted third parties who create public records on behalf of the Board, or manage public records held by the board, are fully aware of and abide by this plan's arrangements.

About the Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) came into force on the 1st January 2013, and requires named public authorities to submit a Records Management Plan (RMP) to be agreed by the Keeper of the Records of Scotland. Integration Joint Boards were added to the Act's schedule by the Public Bodies (Joint Working) (Scotland) Act 2014. This document is the Records Management Plan of Moray Integration Joint Board.

About Integration Joint Boards (IJBs)

The integration of health and social care is part of the Scottish Government's programme of reform to improve care and support for those who use health and social care services. It is one of the Scottish Government's top priorities.

The Public Bodies (Joint Working) (Scotland) Act provides the legislative framework for the integration of health and social care services in Scotland.

It will put in place:

- Nationally agreed outcomes, which will apply across health and social care, in service planning by IJBs and service delivery by NHS Boards and Local Authorities.
- A requirement on NHS Boards and Local Authorities to integrate health and social care budgets
- A requirement on Partnerships to strengthen the role of clinicians and care professionals, along with the third and independent sectors, in the planning and delivery of services

Partnerships will be accountable to Ministers, Local Authorities, NHS Board Chairs and the public for delivering the nationally agreed outcomes.

About Moray Integration Joint Board

Moray Integration Joint Board (the Board) is responsible for the planning and oversight of delivery of health and social care integrated functions for Moray.

The Board's Integration Scheme sets out the functions which are delegated by NHS Grampian and Moray Council to the IJB.

The Board operates as a body corporate (a separate legal entity), acting independently of NHS Grampian and Moray Council. The Board consists of six voting members appointed in equal number by NHS Grampian and Moray Council, with a number of representative members who are drawn from the third sector, independent sector, staff, carers and service users. The Board is advised by a number of professionals including the Chief Officer, Medical Director, Nurse Director and Chief Social Work Officer.

The key functions of the Board are to:

- Prepare a Plan for integrated functions that is in accordance with national and local outcomes and integration principles
- Allocate the integrated budget in accordance with the Plan
- Oversee the delivery of services that are within the scope of the Partnership.

Information underpins the Board's over-arching strategic objective and helps it meet its strategic outcomes. Its information supports it to:

- Demonstrate accountability.
- Provide evidence of actions and decisions.
- Assist with the smooth running of business.
- Help build organisational knowledge.

Good recordkeeping practices lead to greater productivity as less time is taken to locate information. Well managed records will help the Board make:

- Better decisions based on complete information.
- Smarter and smoother work practices.
- Consistent and collaborative workgroup practices.
- Better resource management.
- Support for research and development.
- Preservation of vital and historical records.

In addition we are more accountable to the public now than ever before through the increased awareness of openness and transparency within government. Knowledge and information management is now formally recognised as a function of government similar to finance, IT and communications. It is expected that the Board is fully committed to creating, managing, disclosing, protecting and disposing of information effectively and legally.

14 Elements

The Records Management Plan consists of 14 elements:

- Element 1: Senior management responsibility:
- Element 2: Records manager responsibility:
- Element 3: Records management policy statement:
- Element 4: Business classification
- Element 5: Retention schedules
- Element 6: Destruction arrangements
- Element 7: Archiving and transfer arrangements
- Element 8: Information Security
- Element 9: Data protection
- Element 10: Business continuity and vital records
- Element 11: Audit trail
- Element 12: Competency framework for records management staff
- Element 13: Assessment and review
- Element 14: Shared Information

Elements 1, 9, 13 and 14 are covered below.

The remaining 10 elements are all evidenced through the Moray Council's RMP; this is available on the Council's website: http://www.moray.gov.uk/moray_standard/page_92812.html. The Council's RMP was approved by the Keeper of the Records of Scotland 18th November 2014.

Evidence:
Appendix 1 – Letter confirming shared resources Nov 2018

Element 1: Senior Management Responsibility

The Records Management Plan has the backing of Moray Integration Joint Board and the Chief Officer.

The Senior Manager within Moray IJB with overall strategic responsibility for Records management is:

Pam Gowans,
Chief Officer.

Moray Council HQ,
High Street,
Elgin,
IV30 1BX

The Chief Officer is also the Board's Senior Information Risk Officer (SIRO)

Evidence:
Appendix 2 – Letter of Support from Chief Officer, MIJB, Nov 2018

Element 9: Data Protection

The Board, as a data controller, has registered with the ICO:

Data Controller: Moray Integration Joint Board
Registration Number: ZA313945
ICO webpage: https://ico.org.uk/ESDWebPages/Entry/ZA313945

The Board's Data Protection Officer (and Moray Council's) is:

Alison Morris,
Records and Heritage Manager, Moray Council

Moray IJB utilise the training and guidance that are available through the Council. The Council's FOI Team coordinate requests for access to information under FOI(S)A, EIRS, and, DPA, including Subject Access Requests. Specific Data Protection training was provided to the Board on Thursday 26th July 2018 by Alison Morris.

Evidence:
Appendix 3 – IJB DPA Training July 2018 PowerPoint
Appendix 4 – Data Protection Policy 2018

Element 13: Assessment and Review

The Act requires authorities to keep their plans under regular review to ensure arrangements remain fit for purpose. This plan will be reviewed periodically (or sooner if new legislation, codes of practices or national standards are to be introduced).

The Board will produce an annual report highlighting information on the RMP, particularly for elements 9 and 14 to ensure that ICO registration and compliance with DPA, including refresher DPA training, is maintained. Statistics on FOI and SAR requests will also be included. This report will be produced by the Records and Heritage Manager with assistance from HSCM Management and Legal.

Information on relevant updates to the Moray Council's RMP will be conveyed to the Board as appropriate.

Element 14: Shared Information

The Board has numerous partnerships and working relationships with organisations such as Moray Council, NHS Grampian and, of course, Health and Social Care Moray.

Previously the ICO's Data Sharing Code of Practice has been observed (https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf) and once this is updated the new version will also be observed. All Information Sharing Protocols or Data Sharing Agreements are verified with either Legal or the Records and Heritage Manager.

The majority of documents produced by the Board are publically available. These primarily consist of minutes and reports, as well as guidance on the Board's publication scheme and how to complain. These are all available on the Board's webpages, hosted by Moray Council, http://www.moray.gov.uk/moray_standard/page_100266.html

It is important that the 'ownership' of shared information is clearly established, especially where third party partners or contractors are involved and that the Board's Records Management Plan applies to all third parties who produce or supply information to the council.

List of Appendices

Appendix 1 – Letter confirming shared resources Nov 2018
Appendix 2 – Letter of Support from Chief Officer, MIJB, Nov 2018
Appendix 3 – IJB DPA Training July 2018 Powerpoint
Appendix 4 – Data Protection Policy 2018

APPENDIX 1

Education and Social Care

Alison Morris
Records & Heritage Manager
Elgin Library, Cooper Park, Elgin, Moray, IV30 1HS
Telephone: 01343 562633
Email: alison.morriis@moray.gov.uk
www.moray.gov.uk

Our Ref: Moray IJB RMP Evidence 1
9th November 2018

Dear Keeper of the Records of Scotland,

Moray Integration Joint Board Records Management Plan

Since the creation of the Moray Integration Joint Board (the Board) and the establishment of Health and Social Care Moray there has been a pooling of resources and a combined effort to give these entities the best foundations possible.

The Board and Moray Council shared services such as Legal support, ICT support, administrative services as well as FOI and Records Management assistance. Given this shared working platform it has been reasonable that certain policies and procedures have been shared or replicated, especially within Records and Information Management.

The Council's Records Management Plan (RMP) is currently publically available online, please see: http://www.moray.gov.uk/moray_standard/page_92812.html. This was originally approved by your predecessor 18th November 2014. As a side matter I would like to highlight that the Council's RMP is due for a thorough review in the next year and potential timescales for this have already been discussed with your team.

There are four elements of the Board's RMP that are specifically discussed in their RMP, these are Elements 1, 9, 13 and 14. The remaining elements are already covered by the Council's RMP Elements, as a whole these ensure that Records Management policies, procedures and good practices are utilised for all documents from creation to destruction. A further suite of guidance and advice is available for IJB Officers on the Council's Records Management and Information Security pages. Furthermore, as the Data Protection Officer for both the Council and the Board there is consistent approach on Data Protection, with the underlying message that good records management is the foundation.

Moray IJB emulates the Council's desire for transparency with publishing the vast majority of records they produce. These are available on their pages: http://www.moray.gov.uk/moray_standard/page_100266.html and their FOIs are published alongside the Council's here: http://www.moray.gov.uk/moray_standard/page_62338.html .

With regard to Element 7, as yet no records about or from the Board have been transferred to the Local Heritage Service. The Local Heritage Service covers local heritage information as well as Archival records, and, although run by the Council it is also the repository for a wealth of other organisations too. The reason for this is that records that will be retained for historical value are currently all available online as part of the Board's webpages. A digital archive will be developed to house the key records of the Board in due course.

As Health and Social Care Moray grows it is not anticipated that the Board will alter significantly, however, as both evolve there is scope that in future more of the Board's RMP's elements will be tailored to meet their needs. As such an annual report will be produced to highlight any changes and demands to be addressed; this will ensure that the Board's RMP and records management practices remain relevant and organic.

If there is any further information required or clarifications desired please feel free to contact myself or the IJB Officers.
Yours sincerely,

Alison Morris
Records & Heritage Manager

Health & Social Care Moray

Pam Gowans
Chief Officer
Health & Social Care Moray
Moray Council HQ
High Street
ELGIN IV30 1BX
01343 563552
pamela.gowans@moray.gov.uk
www.hscmoray.co.uk

Your ref:
Our ref:

21 November 2018

Keeper of the Records of Scotland
National Records Scotland
HM General Register House
2 Princes Street,
Edinburgh
EH1 3YY

Dear Keeper

Public Records (Scotland) Act 2011 – Moray Integration Joint Board Records Management Plan

The Public Records (Scotland) Act requires Moray Integration Joint Board to produce and follow a records management plan. This letter of support is Appendix 2 of that Plan.

I confirm that as Chief Officer I have overall responsibility for the Moray Integration Joint Board's Records Management Plan, which has my full support and that of the Board. I will be responsible for ensuring its implementation. As Chief Officer I am also the Board's Senior Information Risk Owner (SIRO).

I also fully endorse the utilising of shared resources with Moray Council. This approach is both practical and gives reassurances that good Records Management practice is already being followed; thus encouraging it to be emulated by the Board as well as by Health and Social Care Moray.

The Board will manage its records in accordance with good records management practices, standards and guidance issued by government, The National Records of

Scotland, the Information and Records Management Society, Archives and Records Association, the Scottish Council on Archives, and, British and International standards.

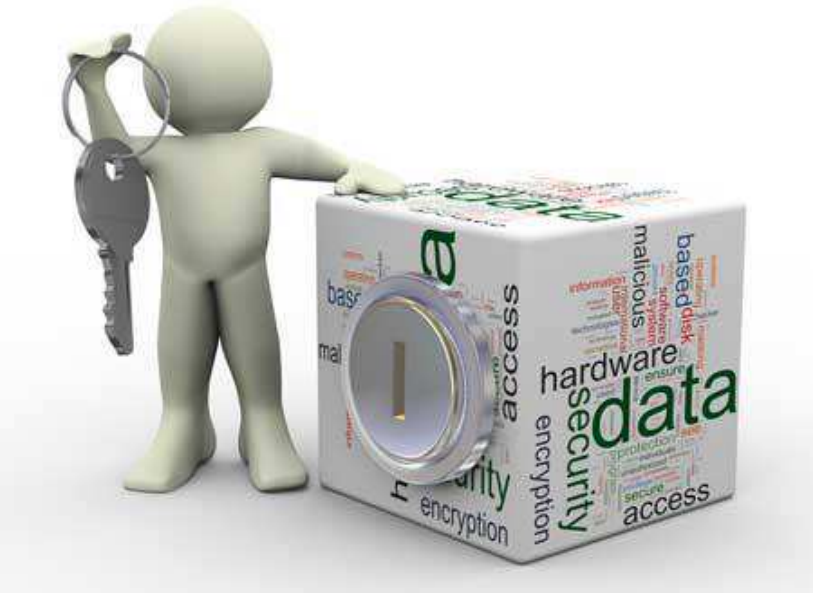
In following good practice the Board will ensure it has the confidence of the public in our records and information management, and, that we comply with legislation including the Data Protection Act, the Public Records (Scotland) Act, Freedom of Information (Scotland) Act and other access to information legislation.

Yours sincerely,

Pam Gowans
Chief Officer

APPENDIX3

Data Protection Legislation
&
Moray IJB



DPA & GDPR

* Data Protection Act 2018
* General Data Protection Regulation (GDPR)

* Personal Data
  * Special Category Data

Has anything changed?

Yes!

Principles updated
State the **Lawful basis/bases** for processing data – **Privacy Notices**
Rights of individuals have changed
Accountability; data audits were used to map every process the Council does (also used for producing Privacy Notices). New processes will need to be added
"Privacy by Design" - Data Protection Impact Assessment (**DPIA**)
Designated Data Protection Officer (**DPO**)
Penalties; £500,000 is now up to €20,000,000 (!!!)

However, if we were compliant with good habits and practices before then it should be relatively simple to be compliant now.

DPO

Data Protection Officers are required to be named, provide expert advise to the data controller, be a single point of contact with the ICO, sign off DPIAs, investigate breaches and have organisational oversight on all Data Protection matters. DPOs must have suitable resources provided to complete their responsibilities.

Moray IJB's and Council's DPO is Alison Morris, Records and Heritage Manager
records@moray.gov.uk
NHS Grampian's DPO is Roohi Bains, Information Governance Officer
nhsg.dpo@nhs.net

Legal support, FOIs etc all done inhouse therefore DPO inhouse too.

IJB primarily holds information already publically available; DPA is about Personal Info.

Principles;

1 - Processed lawfully, fairly and in a transparent manner.
2 - Collected for specified, explicit and legitimate purposes. (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is ok)
3 - Adequate, relevant and limited.
4 - Accurate and, where necessary, **kept up to date**; errors are **erased or rectified** without delay.
5 - Kept no longer than is necessary (stats, historical archiving exempt).
6 - 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.

Plus GDPR; **Accountability**

Legal Basis/Bases

At least one of these must apply whenever we 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: (note that 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).

Rights of Data Subjects

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 rights may be exercised, how to submit a Subject Access Request (SAR), and, when a right does not apply.

DPIAs

Potential data protection and privacy concerns must be **identified** throughout the lifespan of processes and projects. These should be recorded and mitigations put in place to prevent any DPA breaches.

e.g. a risk could be that info is stored outside Europe, e.g. USA. Privacy Shield currently mitigates this, however, it is right to flag it as a concern.

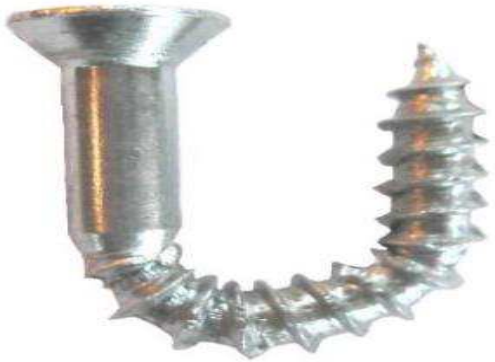
DPIAs must be signed off by the DPO. If risks cannot be mitigated then either the processes or projects cannot go ahead, or, if it does go ahead the ICO should be consulted.

Guidance is available on the Intranet

What to do if it all goes wrong…

We now have **72 hours** to report a breach to the ICO.
All known and reasonably suspected DPA breaches must be highlighted to line managers and the DPO immediately. The DPO will investigate, make the informed decision as to whether to inform the ICO and be the single point of contact. Contact databreach@moray.gov.uk or Alison directly

Data Breach reporting Guidance is available:
http://intranet.moray.gov.uk/Information_management/information_security.htm



Everyday DPA

* Locking computers (window + L)
* Initials in diaries
* Don't leave personal info in voicemails
* Use bulldog clips/elastic bands/envelopes etc
* Only take the information you need with you
* Check e-mail addresses, telephone numbers, postal addresses etc
* Update details on systems (e.g. Carefirst)
* Check your surroundings – e.g. is supermarket the right place for that conversation, should you be making certain comments over the phone in a crowded office?
* Verify who has a right to info
* Keep work in work times.
* Watermarks/indicators for who has a copy of a report.
* Proof read and remember that one day the person might request to see their information: keep it professional.
* BE AWARE AND MINDFUL

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	Alison Morris, Records and Heritage Manager
Consultees	Information Assurance Group: including: Mike Alexander, ICT Security Officer Sheila Campbell, Principal Librarian Sean Hoath, Senior Solicitor Atholl Scott, Internal Audit Manager Graham Jarvis, Acting Corporate Director (Education & Social Care) Scott Reid, GDPR Project Officer Joan Wood, 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

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