Data Protection Guide:
DPA 2018 and GDPR

Information Assurance Group

August 2018

Version 1.1

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

Document Control Sheet

Title:	Data Protection Guide 2018						
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 Guide on the updated Data Protection Act 2018 and the General Data Protection Regulation (GDPR), both came into force May 2018.						
RMP	Element 9 - Appendix 25						
Distribution:	Council wide upon approval						
Version	1.0	1.1	1.2	1.3			
Date	June ‘18	Aug ‘18					

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. Introduction

Data Protection legislation was updated May 2018 with the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) coming into force. GDPR is a European directive and applies to all EU member states, whilst DPA is UK specific. They provide frameworks that ensure information is handled properly and gives individuals rights to know how personal information can be collected, used and stored.

The Council's Data Protection Policy is available on the Information Security intranet page.

2. The Data Protection Principles

The DPA 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.

3. Information Commissioner's Office (ICO)

The 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 to penalise organisations that are not compliant; these include criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve substantial fines of up to €20,000,000 (c.£17million).

Guidance and details on action they have taken are available on their website: ico.org.uk.

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

6. Roles and Responsibilities

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.

Information Asset Owners

The Information Asset Owners (IAOs) are the members of the Senior Management Team. Their role is to understand what information is held by their service, 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 (DPO)

The role of the 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 Alison Morris, Records and Heritage Manager, records@moray.gov.uk or Alison.Morris@moray.gov.uk, 01343 562633.

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.

7. Privacy Notices

For every process undertaken there needs to be a privacy notice to clearly communicate which process the information has been requested or collected for, the legal basis for collecting, and, how the collected information will be handled, stored and potentially appropriately shared. The data subject's rights are stated, as well as links to both the Council's retention schedules and the ICO's website.

In due course privacy notices will be available on the Information Management pages of the Council's website so they are always publically available. Since all current privacy notices are automatically generated in response to the GDPR audits they are only available in PDFs.

If a process requires collecting any personal information then a privacy notice must be provided as well. To organise a privacy notice for a new process, or to update on an altered process, please contact the Data Protection Officer, records@moray.gov.uk .

8. Data Protection Impact Assessment (DPIA)

A DPIA is a method to help identify and minimise the data protection risks of a project or process. DPIAs are required for any processes that are likely to result in a high risk to data subjects' interests and will assist the Council in adopting a 'privacy by design' culture.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to data subjects or to communities, whether it is physical, material or non-material. DPIAs will need to become embedded in project development and involve the DPO and, where appropriate, individuals, stakeholders and relevant experts. If a DPIA identifies a high risk that cannot be mitigated then the ICO must be consulted.

Guidance specifically on DPIAs will shortly be available on the intranet but in the meantime please contact the DPO for specific advice.

9. Information Sharing Protocols and Data Sharing Agreements

Both ISPs and DSAs provide frameworks for the secure and confidential collection, control, storage and sharing of information between participating partner agencies or organisations. It contains an agreed set of principles about sharing personal or confidential information, and, enables each organisation to understand the legal powers and circumstances in which it should share information and what their responsibilities are.

The Council already has a number of ISPs and DSAs with key partners such as COSLA, IJB and suchlike. New protocols or agreements should be approved by Legal and those with specific DPA requirements should also have input from the DPO with copies of the signed agreements saved on the Information Assurance shared drive.

10. Formats

Personal information in **all formats** are covered by Data Protection Legislation, including but not limited to: paper, letters, emails, reports, lists, databases, photographs, telephone recordings, CCTV, video, and, spreadsheets. This is regardless of whichever information repository is used for storage, for example; a paper file, notebook, laptop, computer, external hard drive, USB memory stick, mobile phone and so forth.

11. Good Practice/Practical Considerations

It is important to have a workplace culture established where data protection and privacy is embedded, understood and respected. Therefore it is essential to review practises to ensure procedures are as efficient, robust and secure as possible. Below are examples of relatively small working practises that could prevent a data breach, it is certainly not exhaustive and not all examples will be relevant to all;

General:

- Ensure that information is only discussed within a suitable work environment, for example a parent may bump into their child's teacher in the supermarket and wish to talk about their child but that is not the right place for that conversation.
- Be familiar with the legal bases for sharing information that may apply to your department, in certain circumstances there are exemptions where information should be shared, and, only obtain the information required.
- Endeavour to have a clear desk, especially so in open or shared work areas when anybody could potentially walk past your desk.
- Lock your computer when leaving it (remember that staff are liable for all emails or letters sent in their name) and it is quick to lock a computer by pressing 'L' + the windows key at the same time.
- Be familiar with the various permission or consent forms that may have already been signed by service users, e.g. schools send out annual consent forms, and, if a parent has declined to consent that should be easily recorded and respected.
- Keep language clear and professional; remember data subjects have the right to access **all** information about themselves through a Subject Access Request, they can request to see all information that identifies and relates to them whether it is on paper, in emails or computer systems or suchlike.
- Under DPA a person aged 12 or over is presumed of sufficient age and maturity to understand their DPA rights and give consent where required.

Paperwork:

- When sending letters or producing copies of paperwork for meetings it may be suitable to highlight to whom the copy belongs; i.e. Service Users', Pupil's, Professional's Copy. Therefore if a service user accidentally loses their paperwork it is clear that it was the service user who had misplaced their copy; this means we know to offer a new copy as well as ensure our reputation is not tarnished.
- Only take out of the office files or paperwork if it is necessary to do so; ensure that suitable protection is in place to cover any information on display, prevent environmental damage (e.g. rain) and it is secure (e.g. loose pages won't get blown away if dropped, difficult to be stolen)
- Consider a register for recording which files have been taken out and returned to the office. Therefore if a file is missing it is evident when and where it was taken and by whom.
- In diaries, especially if taken outside the office, try to use initials for service users instead of full names/addresses.
- Mark letters and envelopes for the attention of the addressee only and offer the Council's address for return delivery should the wrong addressee receive it.
- Use page numbers that state 'page 1 of 3' so it is clear if a page is missing.
- Ensure relevant contact details are kept up to date, a test email or phone call can always be used before sending information if there is any uncertainty.
- It is worth verifying a service user's identity, power of attorney or parental rights and responsibilities before releasing personal information, especially so if the information relates to a child or third party.

Emails:

- Ensure that email addresses are correctly written; including the last part as .co.uk is different from .com, .gov.uk or .org.uk.
- When you have multiple email addresses for the same name or person ensure that Outlook has not defaulted to the most recent email address.
- Do not give out your own personal email address for work purposes and do not email yourself work documents.
- When sending an email to multiple recipients, especially if they are personal email addresses, ensure to utilise the 'bcc' (**B**lind **C**arbon **C**opy) function so not to share the personal email addresses.
- Note that emails sent within the Council's firewall can be recalled, however, any that have left the network (i.e. sent outwith the Council) cannot be recalled. Emails sent from shared inboxes cannot be recalled, whether internal or externally sent.
- Be aware when forwarding emails that there could be information in earlier emails that is unsuitable to share, similarly with attachments.
- Keep email inboxes tidy and delete emails when they are no longer required or useful. If an e-mail is required to be kept as part of a decision making process it should be suitably saved, for example into SharePoint or on a shared system.
- Avoid using scanned images of signatures as these can easily be lifted and reused without knowledge or consent.

Telephones:

- Be aware of your environment when discussing any personal details on the phone, for example an open plan office is not the best place to repeat back bank details of a service user or to discuss their criminal record. If such sensitive details have to be discussed then, where possible, organise a suitable space and time to do so.

- When leaving voicemails outwith the Council it is recommended to only leave your name and number with a request for the person to contact you; do not discuss the topic as you cannot guarantee the voicemail will be heard by the intended recipient.
- Be aware of your own personal information as well. For example; if on your lunch break you are on your mobile ordering a washing machine remember that others near you do not also need to hear your bank details, your home delivery address and that you won't be in over the weekend.
- If asked for sensitive information over the phone the option is always available to verify the contact details already in the system and then return the call when you have prepared the relevant information.

Storage:

Information in any format should always be held securely and in the correct repository;

- Current paperwork should be kept in suitable storage; in files, in desk draws, cabinets and suchlike.
- Semi current paperwork can be transferred to the Closed Records Store (see below for details) or handled by the Mailroom.
- Pen drives and external hard drives should not be used to transport information unless it is vital to do so, and, the device is encrypted and password protected.
- Where possible, rather than sending attachments instead send links to documents in shared drives and systems such as SharePoint.
- Laptops and other devices should be transported and kept securely.
- When transporting information, such as a laptop or file, ensure that it is not left unattended or obvious, for example do not leave files with names or details exposed on the passenger seat of a car.
- Information should not be held outside of work environments unless it is absolutely necessary; in such situations it is important to record what information is housed where and all reasonable steps that have been taken to protect it.

12. Retention

Information must only be kept as long as necessary, as per the DPA principles, and in accord with the Council's Retention Schedules.

13. Confidential Waste

The confidential waste contract ensures that there are numerous receptacles available for confidential waste. These are collected regularly then securely shredded and recycled. Departmental shredders should not be used. Further information on the Council's Confidential Waste policy, location of Shred-it bins and how to obtain extra bags for ad hoc collections is available on the intranet: Records Management > Confidential Waste

This contract is due for renewal September 2018, as such Shred-it bins may be replaced with other receptacles at this time.

14. Closed Records Store (CRS)

Semi-current paper files can be transferred to the CRS for storage until the end of their retention period, at which point sign off will be required for either secure destruction, extending the retention period or recommending transfer to archives.

More information is available on the intranet: Records Management > CRS

15. Breaches

Information on how to report a known or suspected data breach is available on the intranet: Data Protection Breach Management.

16. Training

All employees will be provided with training in basic data protection legislation and practice as soon as reasonably practicable after starting to work for the Council. This is available through CLIVE as an online module (simply search for 'GDPR') 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.

17. Further Information and Contacts

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

Alison Morris, Records and Heritage Manager, records@moray.gov.uk or Alison.Morris@moray.gov.uk, 01343 562633. Or,

Information Co-ordinator, 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