mental welfare commission for scotland

Policy Title: Data Protection Policy	**Policy Number:** IG-POL-03
Issue Number: 13	**Date of first issue:** June 2004
Date of last review: February 2025	**Date of next review:** February 2027
Lead person: Information Governance Manager	**Approved by:** Board
	Date approved: 25/02/2025

General Note

The Mental Welfare Commission acknowledges and agrees with the importance of regular and timely review of policy statement and aims to review policies within the timescales set out.

New policies will be subject to a review date of no more than one year from the date of first issue.

Reviewed policies will have a review date set that is relevant to the content (advised by the author) but will be no longer than three years.

If a policy is past its review date, then the content will remain extant until such time as the policy review is complete, and the new version published.

1. Policy Statement

The Mental Welfare Commission for Scotland needs to collect and use a variety of sensitive and personal information about people to fulfil its statutory functions and other operational duties. This information includes data on users of mental health, learning disability and social care services and their carers; current, past and prospective employees; suppliers; clients/customers; and others with whom it communicates. All such personal information shall be dealt properly and securely no matter how it is collected, recorded and used.

The Commission will comply with its obligations under UK GDPR and the UK Data Protection Act 2018 and any other relevant legislation. We will observe the principles of the Caldicott Guardian. The Commission will ensure that it continues to treat personal information with due care and diligence.

2. Scope

This policy applies to all employees, agency workers including those attached to the Commission as part of their professional training, secondees and contractors.

In relation to GDPR/DPA, Board members are expected to abide by the Commission's policies and procedures in relation to data protection, IT and information risk produced by the Commission and also to comply with the Board Code of Conduct.

This policy applies to all situations where we process (collect, store, use, share) personal data about individuals. It includes, but is not limited to information processed electronically, on paper, in emails, in employee files, in internal memos, in photographs and on audio equipment.

The Commission remains the data controller of the records produced by the National Confidential Forum (the NCF). The NCF was established as a Committee of the Commission in 2014 under the Victims and Witnesses (Scotland) Act 2014 and came to an end on the 28 June 2021 under the terms of the Redress for Survivors (Historical Child Abuse in Care) (Scotland) Act 2021. During its lifespan, the NCF was a committee of the MWC and did not exist as a separate legal entity from the Commission. The NCF's core function was to receive and listen to testimony from those who were in institutional care as children.

3. Definitions

Personal data is defined as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.'

Special categories of data Special (defined by Article 9 of the UK General Data Protection Regulation (UK GDPR)) and sensitive data (defined by section 35 of the DPA 2018) is personal data which reveals:

- racial or ethnic origin political opinions,
- religious or philosophical beliefs or trade union membership,
- the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual,
- the processing of data concerning health,
- the processing of data concerning an individual's sex life or sexual orientation.

Criminal offences and criminal conviction. Article 10 UK GDPR applies to the processing of personal data relating to criminal convictions and offences or related security measures. In addition, Section 11(2) of the DPA 2018 provides that criminal offence data includes data which relates to the alleged commission of offences and related proceedings and sentencing. Information about victims and witnesses of crime is also included in the scope of data relating to criminal convictions and offences.

4. Roles & responsibilities

Chief Executive

4.1 The Commission's Chief Executive has overall responsibilities for data protection within the Mental Welfare Commission. The Chief Executive is the accountable officer for data protection matters and is ultimately responsible for ensuring data protection practices are observed at the Commission.

Head of Culture & Corporate Services

4.2 As the Senior Information Risk Owner (SIRO), this postholder has responsibility for ensuring information assets (records) are processed in a safe, fair, and lawful manner. This responsibility extends to all records held by the Commission, in whatever format and for whichever purpose.

4.3 Data Protection Officer (DPO) (Information Governance Manager)
At the Commission, the DPO is the information governance manager.
The DPO holds a key advisory and monitoring role in relation to the use and management of personal data. Their role and responsibilities are defined under UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. developing policy, procedures and guidance in respect of Data Protection legislation. The DPO reports key findings and recommendations to the Executive Leadership Team.

4.4 Information Asset Owners (IAO) are responsible for maintaining, registering and safeguarding information assets. IAOs also have a responsibility to ensure compliance with data protection law within their business area.

4.5 Caldicott Guardian
The caldicott guardian has responsibility regarding the use of patient identifiable information. They are responsible for ensuring use of patient identifiable information is legal, ethical, and appropriate, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

4.6 Audit, Performance & Risk Committee:
The Committee will monitor and scrutinise the adequacy and effectiveness of arrangements in place for data protection, information management and security.

4.7 Commission staff.

All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work and to be fully aware of their duties and responsibilities under the Data Protection Legislation.

All staff are responsible for:

• familiarising themselves with the implications of data protection in their job
• adhering to this policy and supporting guidance.
• reporting any activities that do not comply with this policy.
•seeking guidance and advice where necessary.
• checking that any personal data that they provide is accurate and up to date;
• checking any information that the Commission may send out from time to time, giving details of information that is being kept and process.

All staff are bound by a legal duty of confidentiality to protect personal information they may come into contact with during the course of their work. This is not just a requirement of employee's contractual responsibilities but also a requirement within the Data Protection Act 2018 (DPA 2018), the Common Law Duty of Confidentiality and any other appropriate professional standards of confidentiality.

Failure to comply with this policy could result in disciplinary action. It is mandatory for all staff to read and understand their responsibilities in accordance with the principles and practice set out in the reference document section.

4.8 The table below describes the required competency level for staff

Level of competency	Description of competency	Who covers that role at MWC
Advanced knowledge and skills	Develops policy, procedures and practice in own organisation as it relates to information governance. Maintains own awareness of changes in legislation, case law, best practice, policy and guidance.	Information Governance Manager Caldicott Guardian
Intermediate level	Applies data protection principles and key legislation to own work role and work of others.	Senior Managers

	Monitors compliance with policies/procedures	Practitioners Corporate Services Managers Casework Managers Executive Leadership Team & CEO
Foundation level	Understanding of data protection principles and awareness of key legislation and policy. Understanding of the need for secure and confidential information handling in relation to own work role. Awareness of sources of information, referral, advice and guidance (including local policies). Store, transport and transfer health records and other personal or other sensitive data securely and effectively.	All staff

5 Operational system

The UK General Data Protection Regulation (UK GDPR) governs the processing of personal data of individuals by 'data controllers', such as the Commission. The Data Protection Act 2018 enshrine the regulation into UK legislation.

Article 5.1 of the UK General Data Protection Regulation outlines the six data protection principles (detailed below) which must be adhered to when processing personal data. Article 5.2 states that controllers must be able to demonstrate compliance with paragraph 1.

5.1 Data protection principles

We must comply with the UK GDPR, which requires that data is collected and used fairly, stored safely and not processed unlawfully. In particular, the Commission will comply with the following GDPR principles while processing data subjects' data:

1. **Lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner.

2. **Purpose limitation.** Data shall only be obtained and processed for one or more specified, explicit and legitimate purposes.

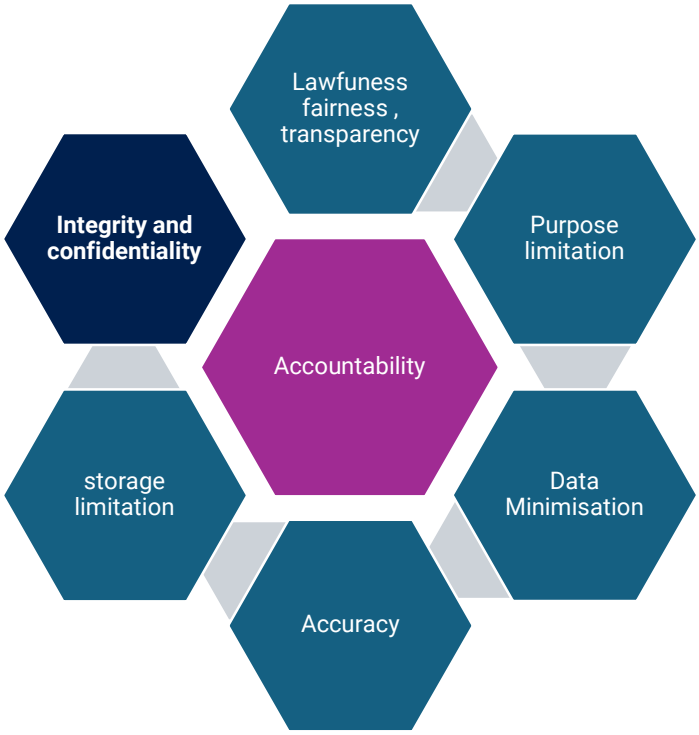
3. **Data minimisation.** Data should be adequate, relevant and not excessive for those purposes.

4. **Accuracy.** Personal data shall be accurate and, where necessary, be kept up to date.

5. **Store limitation.** Data should not be kept for longer than is necessary for the original purpose for which it was obtained.

6. **Integrity and confidentiality.** Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7. **Accountability and governance**. The Commission must have in place appropriate technical and organisational measures able to demonstrate compliance with the UK GDPR.



5.2 Implementation

In order to meet the requirements of the principles, the Commission will:

- Establish and maintain an Information Asset Register with each identified asset having an owner who is accountable for safely managing assets in their domain.
- Ensure that there is an appropriately qualified Data Protection Officer (DPO) as required under GDPR.
- Fully observe conditions regarding the fair collection and use of information.
- Meet our legal obligations to specify the purposes for which information is used and establish the legal basis for the process in accordance with GDPR.
- Collect and process appropriate information, but only to the extent that it is needed to fulfil statutory responsibilities or operational needs.
- Ensure that information is of adequate quality.
- Control the length of time information is held in line with the Commission's, Records Management Policy (IG-POL-01)
- Ensure that the rights of people about whom information is held can be fully exercised under GDPR. (website privacy policy). These include: the right to be informed that processing is being undertaken, the right of access to personal information, the right to prevent processing in certain circumstances and the right

to rectify, block or erase information which is regarded by both parties as wrong information.

- Ensure that personal information is not transferred abroad without suitable safeguards.

- Take appropriate technical and organisational security measures to safeguard personal information.

- The Commission will ensure that privacy by design is satisfied and data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests are carried out.

- Ensure that the Commission only shares personal information with the relevant agents lawfully and securely by conducting risk assessment prior to sharing information further, following data sharing protocols and forms.

5.3 **Organisational Issues**

- The Commission will ensure that it complies with any directive from the ICO regarding the registration process and pay the appropriate fee in accordance with guidance from the ICO.

- The Data Protection Officer for the Commission is the information governance manager. Scrutiny for data protection at the Commission will be carried out by the Audit, Performance and Risk Committee.

- The Commission will observe the principles of the Caldicott Report and in particular will ensure that there is a nominated Caldicott Guardian. Guidance about the role and responsibilities of Caldicott Guardians is available from NHS Scotland Caldicott Guardians: principles into practice[1] . Caldicott principles are listed in section 5.5.

5.4 **Data protection and individuals' rights**

The Data Protection Legislation provides the following rights for individuals (subject to exemptions):

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object and
- rights in relation to automated decision making and profiling

Individuals also have the right to withdraw consent where given, and the right to complain to the ICO.

Any requests to exercise these rights are forwarded to the DPO for advice.

All the information held about an individual (regardless of where you store that information and its format) is susceptible to be disclosed to the data subject in response to a subject

[1] This NHS guidance is dated 2012 but there have not been any further updates. New Caldicott guardian principles have been introduced since then. Principle 7, "the duty to share information can be as important as the duty to protect patient confidentiality" and Principle 8 "Inform patients and service users about how their confidential information is used". See also National Data Guardian NDG website

access request. Information about individuals must be accurate and up to date and filed in the right place so it can be promptly located. Staff must be able to recognise data subject access requests and forward them to the information governance manager for its prompt processing. All request for personal data will be processed following the CORP-SOP-Data Subject Access Request

Individuals' rights are explained in the Privacy Statement available on the website. There is also a film explaining how we process personal data. About your personal information | Mental Welfare Commission for Scotland (mwcscot.org.uk)

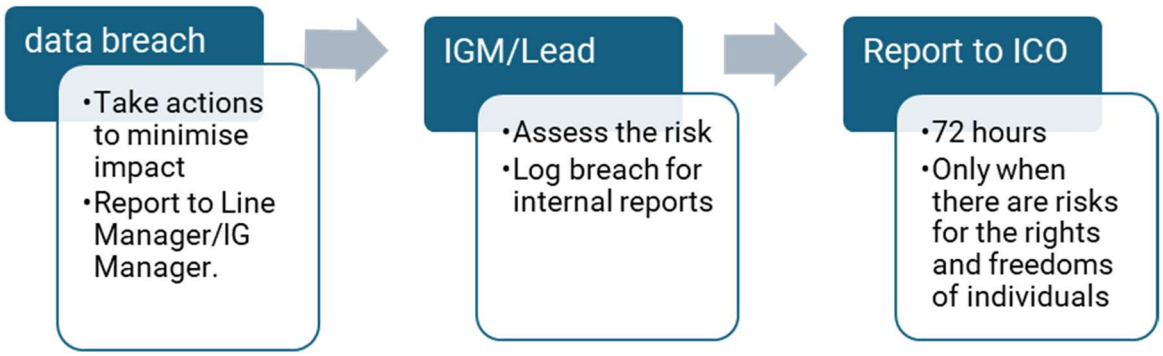
Organisational and technical measures in place to comply with the principles while processing special categories of data are details in section 6.

5.4 **Information loss & obligation to report data breaches to the Information Commissioner's Office (ICO)**

Data breach or an incident involving the security of information held by the Commission, relating to individuals who contact us or anyone working with or for the Commission, must be reported immediately by staff to their line manager and the information governance manager following the instructions in the Data Breach Procedure (CORP-SOP-10)

Under the UK GDPR, reporting serious data breaches is mandatory and must be done within 72 hours of the organisation becoming aware of the incident.

Staff will be asked to provide details about the circumstances of the breach, the type of data involved, who that data relates to and the potential impact on individuals affected.
Staff should also take appropriate actions to retrieve the information that has been lost, where this is practical and not likely to exacerbate the situation (for example, when an email has been sent to the wrong recipient)



5.5 **Caldicott Principles**

In addition to the UK GDPR, staff handling individuals' health and social care records and information should also be aware of and comply with the Caldicott Principles, these are:

Justify the purpose(s) for using confidential information.

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing use regularly reviewed by an appropriate guardian.

Use confidential information only when it is necessary.

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Use the minimum necessary personal confidential data.

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Access to confidential information should be on a strict need-to-know basis.

Only those individuals who need access to confidential information should have access to it, and then only to the items that they need to see.

Everyone must understand their responsibilities.

All those who handle patient-identifiable information should be made aware of their responsibilities and obligations to respect the confidentiality of patients and service users.

Understand and comply with the law.

Every use of patient-identifiable information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

The duty to share information can be as important as the duty to protect patient confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of their patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Inform patients and service users about how their confidential information is used.

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information – in some cases, greater engagement will be required.

If you have any concerns about disclosing or sharing patient or colleague information you must discuss this with your line manager in the first instance or, if you are uncertain whether disclosure of information can take place, contact the Caldicott guardian (Commission's Executive Director – Medical). When the information relates to social work data, consider discussing the concerns with the Executive Director (social work).

6 Appropriate Policy Document and additional safeguards

This section has been developed to meet the requirements in the Data Protection Act 2018, part 4 of Schedule 1 which requires that an appropriate policy document is in place in relation of the processing of personal data in reliance on a condition described in **part 1, 2, and 3 of Schedule 1 (** Part 1- employment, health and research etc; Part 2- substantial public interest; Part 3- additional conditions relating to criminal convictions)

An appropriate policy documents is a document which:

(a)explains the controller's procedures for securing compliance with the principles in Article 5 of the 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.

At the Commission we maintain a record of our processing activities in accordance with Article 30 of the UK GDPR which has been merged with the business classification scheme and retention policies.

6.1 **PRINCIPLE 1. Lawfulness, fairness and transparency.** Processed lawfully, fairly and in a transparent manner in relation to individuals. Article 5 (1) (a) DPA 2018 and Article 6 UK GDPR

6.1.1 **Conditions for processing special categories of data and criminal convictions.**

The Mental Welfare Commission is a statutory body with statutory functions. As part of the Commission's statutory and corporate functions, we process special categories of data and occasionally criminal offence data under the following UK GDPR Articles:

i - Article 9(2) (b) – where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Commission or the data subject in the field of employment and social security and social protection law.

This includes information about staff health and wellbeing, ethnicity sickness absences and political activity declarations and other human resource management purposes. Further information about this processing can be found in the staff privacy statement .

ii- Article 9 (2) (g) -reasons of substantial public interest.

Most of our processing is necessary so we can carry out our statutory duties set out in the Mental Health (Care and Treatment) (Scotland) Act 2003 and Adults with Incapacity (Scotland) Act 2000. Further information about this processing can be found in the Privacy Statement available on the website.

iii. Article 9 (2) (j) for archiving purposes in the public interest. The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.

An example of our processing is the transfers we make to the National Archives of Scotland under the Public Records (Scotland) Act 2011.

iv. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

Examples of our processing include processing relating to any employment tribunal or other litigation.

v. Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information.

9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of our processing would be using health information about a member of staff in a medical emergency, or we need to share information about an individual because they are in imminent risk, for example a suicidal caller.

We process criminal offence data under Article 10 of the UK GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations or when this information is part of the health records.

6.2.2 **DPA 2018. Schedule 1 conditions for processing.** Processing of personal data in reliance on a condition described in part 1 and 2of Schedule 1.

PART 1 Schedule 1

The Commission process special category data for the following purposes in Part 1 Schedule 1:

- paragraph 1 – employment, social security and social protection
- paragraph 4 – research, archiving, scientific, historical or statistical purposes carried out in accordance with Article 89(1) and is in the public interest

Employment, social security and social protection law.

All processing is for the first listed purpose and might also be for others, depending on the context. The Commission processes special category data for human resources when the processing is necessary for the purpose of performing or exercising rights which are imposed or conferred by law to the Commission as a data controller or the data subject in connection with employment, social security or social protection.

Archiving purposes in the public interest

Under Article 9(2)(j) of the UK GDPR, the Commission may process special category data where it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on UK and EU or EU member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

PART 2 Schedule 1

Substantial public interest

Section 10(3) of the DPA 2018 sets out that for processing special categories of personal data and criminal offence data for reasons of substantial public interest under Article 9(2)(g) of the UK GDPR, that processing must meet one of the conditions set out in Part 2 of Schedule 1. The following conditions set out in the following paragraphs of Part 2 of Schedule 1 to the DPA 2018 are relevant for the Commission, but there could be others, depending on the context

- Paragraph 6(1) and (2)(a) statutory, etc. purposes.
- Paragraph 8(1) equality of opportunity or treatment
- Paragraph 9 (1) racial and ethnic diversity at senior levels of organisations.
- Paragraph 10(1) preventing or detecting unlawful acts
- Paragraph 11(1) and (2) protecting the public against dishonesty
- Paragraph 12(1) and (2) regulatory requirements relating to unlawful acts and dishonesty
- Paragraph 18 (1) Safeguarding of children and of individuals at risk

Criminal offence data – We process criminal offence data for the following purposes in Parts 1 and 2 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6 – statutory etc and government purposes ie necessary for the exercise of the function conferred on a person by an enactment or rule of law, or exercise of a function of the Crown, a Minister of the Crown or a government department

5.1.2 **Fairness and transparency**

The Commission will ensure that the data subject receives full privacy information so that any processing is transparent.

The Commission will provide clear transparent information to all those who provide personal data to us in the privacy statement available on the website, our short film explaining how we process personal data and directly to individuals during our visits.

Commission's employees have access to our employee's privacy notice.

In relation to all such processing, the Commission will comply fully with their duties under the UK GDPR and the DPA 2918 in relation to the rights of the data subject.

The Commission will observe the principles of the Caldicott Report and will ensure that there is a nominated Caldicott Guardian. Guidance about the role and responsibilities of Caldicott Guardian is available from NHS Scotland Caldicott Guardians: principles into practice[2], The Caldicott Guardian shall be the Chief

[2] This NHS guidance is dated 2012 but there have not been any further updates. New Caldicott guardian principles have been introduced since then. Principle 7, "the duty to share information can be as important as the duty to protect patient confidentiality" and Principle 8 "Inform patients and service users about how their confidential information is used". See also National Data Guardian NDG website

Executive, except where the post-holder is not medically qualified, when the Executive Director (Medical) shall be nominated as Caldicott Guardian.

6.2 **PRINCIPLE 2. Purpose limitation. Article 5 (1) (b)**

The Commission will not process personal data for purposes that are incompatible with the purposes for which it is collected and to fulfil our statutory functions set out in legislation.

The Commission will ensure that any changes to the processing of data are considered through a thorough Data Protection Impact Assessment (DPIA) process.

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.

When the Commission shares special category data, sensitive data or criminal offence data with another controller, processor or jurisdiction, we will ensure that the sharing is necessary and proportionated and there is a legal condition that justifies the sharing. We will ensure that data transfers are compliant with relevant laws and regulations and use appropriate international treaties, data sharing agreements and contracts.

6.3 **PRINCIPLE 3. Data Minimisation. Article 5 (1) (c)**

The Commission collects personal data that is adequate, relevant and limited to the purposes for which it is processed. We ensure that the information we process is necessary for and proportionate to our purposes.

A data protection impact assessment must be completed and submitted with the Project initiation documents describing the information to be collected and processing and why the information is necessary and relevant for the purpose of the project.

6.4 **PRINCIPLE 4. Accuracy. Article 5 (1) (d)**

Personal data shall be accurate and, where necessary, kept up to date. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay.

- *The Commission will carry out data quality exercises as part of standard practice. For example, data checking against national systems available to the NHS"*
- *Include data accuracy clauses within agreements with other organisations where data sharing takes place.*
- *Have processes in place to manage the rectification of data errors in records*

6.5 **PRINCIPLE 5. Storage limitation. Article 5 (1) (e)**

The Commission controls the length of time information is held in line with the **Commission's, Records Management Policy** (IG-POL-01) and Business Classification Scheme with associated retention periods and in accordance with its approved Records Management Plan.

At the Commission, retention policies and business classification scheme have been merged in a single document.

Once we no longer need personal data it will be deleted, put beyond use or anonymised.

Our retention schedule is reviewed regularly and updated when necessary.

6.6 **PRINCIPLE 6. Integrity and confidentiality. Article 5 (1) (f)**

The Commission have put in place appropriate technical, physical and managerial procedures to safeguard and secure the information we collect about individuals. We have strict security standards, and all our staff and other people who process personal data on our behalf receive regular training about how to keep information safe. We limit access to personal information to those employees, or third parties who have a business or legal need to access it.

Third parties or contractors that the Commission engages will only process personal information on our instructions or with our agreement, and where they do so they have agreed to treat the information confidentially and to keep it secure.

Measures The Commission obtained the Cyber Essentials Accreditation for the first time in 2018 since it become compulsory. This accreditation needs to be renewed every 12 months.

The government-owned Cyber Essentials scheme aims to help organisations of all sizes defend themselves against the most common cyber threats and reduce their online vulnerability. It defines a focused set of five technical controls which offer cost-effective, basic cyber security, via two levels of certification:

- **Cyber Essentials (CE):** The basic verified self-assessment option
- **Cyber Essentials Plus (CE Plus):** As above, but independent technical verification is also carried out by the Certification Body

Cyber Essentials is operated in partnership between the Department for Science, Innovation and Technology (DSIT) and the National Cyber Security Centre (NCSC). It is delivered through the IASME Consortium Ltd. (IASME).

Controls include but are not limited to:

- **Staff training**. Induction and mandatory annual Information Security and data protection Training for all staff within a 2-year training cycle.

- Acceptable use of IT equipment and systems defined in IT policies and operating procedures signed by all users of the Office's systems.

- Role Based Access Controls, limiting the Office's system users to only access those systems necessary for them to perform their duties

- Appropriate prevention of the Office's core IT system (e.g. firewalls, malware detection and defence)

- Encryption of data in transit

- Monitoring and/or logging of digital and user activity into, within and out of the Office's systems

- Annual and ad-hoc IT health checks and penetration tests by independent certified test teams; with follow-up treatment of identified vulnerabilities

- Clear desk policy in all departments and at all levels

- Robust procedures for the reporting of any data or potential data breaches.

- Ensure that personal information is not transferred abroad without suitable safeguards.

- Memorandums of Understanding with other relevant agencies in compliance with ICO data sharing guidance and Codes of Practice.

6.7 **Accountability. Article 5 (2)**

To meet the overarching requirement of accountability the Commission will maintain adequate records of our data processing activities and keep evidence of how we comply with the data protection principles:

- Appointing a data protection officer who reports directly to the ELT and the audit, performance and risk committee. The data protection officer for the Commission is the information governance manager

- The Commission maintains a record of processing activities under Article 30 of the UK GDPR.

- We carry out data protection impact assessments where appropriate in accordance with Articles 35 and 36 of the UK GDPR to ensure data protection by design and default.

- Ensuring regular monitoring and maintenance of polices concerning data protection issues. Including but not limited.

    - Data subject Access request procedure.
    - Data breach policy/procedure.

- The Commission maintains a log of requests received for personal information (Subject Access Requests) and has a clear procedure for their processing.

- The Commission keeps a record of all data breaches, actions taken, and lesson learned and has a clear policy for recording processing.

6.8 **Data Protection Impact Assessments**

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. We must do a DPIA for processing that is likely to result in a high risk to individuals.

This includes some specified types of processing. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Our DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- - identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We should consult our data protection officer and, where appropriate, individuals and relevant experts. Any processors may also need to assist us.

If we identify a high risk that we cannot mitigate, we must consult the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, they may issue a formal warning not to process the data, or ban the processing altogether

7. Risk Management

This policy and the arrangements in place will ensure that the Commission will manage personal data as prescribed in the Data Protection Act 2018 (DPA), UK GDPR and related legislation.

A report will be submitted to the Audit, Performance and Risk Committee twice a year with a summary of the actions taken and any significant incidents.

8. Related Documents

- No. 5. IT Security Policy
- CORP – IT code of conduct & Information Risk Management handbook
- No.65. Secure handling use storage retention and disclosure of disclosure information.
- Business Continuity Management Policy
- Records Management Plan
- Data and Information strategy (do we have an approved version).
- Business classification Scheme (BCS) and Retention schedules
    - BCS business support
    - BCS statutory activities
    - Summary retention business support records
    - Summary retention policies statutory activities

PROCEDURES

Data Breach procedure
Data subject Access Request Procedure

9. References

The UK Information Commissioner's Office: http://www.ico.gov.uk/

The British Medical Association: http://www.bma.org.uk

The General Medical Council: http://www.gmc-uk.org

NHS Inform – Includes links to useful leaflets about; consent, confidentiality and how to see health records. http://www.nhsinform.co.uk/rights/publications/leaflets/