SECTION B: DATA PROTECTION

1. INTRODUCTION TO DATA PROTECTION

The Commission recognises the importance of ensuring that personal data is handled in accordance with the requirements set out in the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (GDPR).

Failure by Commission employees to safeguard Personal Data properly might result in disciplinary action being taken.

1.1 Introduction to the Data Protection Legislation (DPL)

The DPL regulates the collection, storage, processing, use (including disclosure) and destruction of information relating to an identified or identifiable living individual.

1.2 The Data Protection Principles

The DPL contains rules which must be followed when processing Personal Data, known as the "Data Protection Principles". These provide that Personal Data must:

(i) **Be processed fairly, lawfully and in a transparent manner.** This means that it must be made clear to data subjects that personal data about them is being processed and the purposes for which it is being processed;

(ii) **Be obtained only for specific, explicit and legitimate purposes and shall not be processed in any manner incompatible with those purposes.** This means that personal data collected for one purpose cannot be used for a different, unrelated purpose;

(iii) **Be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;**

(iv) **Be accurate and where necessary, kept up to date;**

(v) **Not be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed**. This needs to be considered in light of statutory obligations requiring certain data to be kept for certain specified periods of time, further details of which are contained within the Commission's Records Retention Policy; and

(vi) **Kept secure by means of appropriate technical and organisational safeguards.**

2. INFORMATION RELATING TO COMMISSION EMPLOYEES

The Commission uses employee's Personal Data to:

- recruit promote and train employees;
- manage employee's pension scheme and pension forms, sickness records, redeployment and/or career development;
- calculate payroll and the transfer of such data for use by financial employees and independent auditors;
- determine and calculate certain benefits, including superannuation;
- contact next of kin and arrange medical attention in connection with an emergency at work;
- prevent fraud;
- comply with lawful requests from government agencies;
- comply with disciplinary or capability information arising from an employee's conduct, or ability to perform their job requirements; and
- provide references/reports to third parties on request.

3. BASIS AND PURPOSES FOR PROCESSING PERSONAL DATA

Before any Personal Data is processed by the Commission for the first time, the Commission will review the purposes of the particular processing activity and select the most appropriate lawful basis under the DPL. The lawful bases most commonly used by the Commission are that:

- the individual has consented – this is only appropriate where it is not a precondition of a service, no another lawful basis applies and there is no imbalance of power between the Commission and the individual;
- the processing is necessary for performance of or to take steps to enter into a contract with the individual;
- the processing is necessary to comply with a legal obligation – the Commission needs to process certain Personal Data under law;
- the processing is necessary for the Commission to carry out a task in the public interest which is laid down by law or the exercise of the Commission's official authority as laid down by law; or
- the processing is necessary for the Commission's or a third party's legitimate interests – provided that the legitimate interests are not overridden by the interests of the individual.

The Commission will also document the Commission's decision as to which lawful basis applies, to help demonstrate compliance with the Data Protection Principles, and will also include information about the purposes, lawful basis and special condition (if applicable) of the processing within the Commission's relevant privacy notices.

3.1 Processing Special Category Data

Under the DPL, the processing of certain information, known as Special Category Data, is subject to special restrictions. An individual's explicit consent (subject to limitations) is required to hold such data unless there is an exception provided under the DPL. In relation to any queries about whether information held constitutes Special Category Data and if there are any exceptions under the DPL, please refer to the Data Protection Officer.

4. HANDLING OF PERSONAL DATA

The Commission will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions regarding the fair collection and use of Personal Data;
- meet its legal obligations to specify the purpose(s) for which Personal Data is used;
- collect and process appropriate Personal Data and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of Personal Data used;
- take appropriate technical and organisational security measures to safeguard Personal Data;
- ensure that Personal Data is not transferred outwith the EU without suitable safeguards; and
- ensure that the rights of people about whom the data is held are respected and can be fully exercised by them under the DPL and against the Commission.

The Commission will also ensure that:

- there is someone appointed to the role of the Commission's Data Protection Officer;
- everyone within the Commission who is managing and handling Personal Data understands that the Commission is legally responsible for following good data protection practice and complying with the DPL;
- everyone managing and handling Personal Data within the Commission is appropriately trained to do so;
- queries and complaints about handling Personal Data are promptly and courteously dealt with; and
- data processing by third parties on behalf of the Commission is carried out under a written agreement.

In accordance with the Commission's IT Security Policy, the Commission will take steps to ensure that Personal Data is always kept secure against unauthorised or unlawful loss or disclosure and, will ensure that:

- appropriate technical measures, including internet security, anti-virus software and firewalls, are installed and kept up-to-date;
- Personal Data held on computer systems is protected by the use of secure passwords and mandate strong password security; and
- passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other associates or agents processing Personal Data for and on behalf of the Commission as processors must enter into a contract that provides (as a minimum) that they:

- only act on the written instructions of the Commission (unless required by law to act without such instructions);
- ensure that people processing Personal Data on behalf of the Commission are subject to a duty of confidence;
- only engage a sub-contractor to process Personal Data on behalf of the Commission with the prior consent of the Commission and a written contract;
- assist the Commission in responding to requests from data subjects seeking to exercise their rights under the DPL;
- assist the Commission in meeting its obligations under the DPL in relation to security of processing, the notification of Personal Data breaches and data protection impact assessments where applicable;
- delete or return all Personal Data to the Commission as requested at the end of the contract;
- allow data protection audits and inspections by the Commission of Personal Data held on its behalf (if requested) to ensure that both parties are meeting their requirements under the DPL and tell the Commission immediately if asked to do something that infringes the DPL; and
- indemnify the Commission against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

5. DOCUMENTATION AND RECORDS

The Commission keeps written records of processing activities, including:

- the name and details of the Commission;
- the purposes of the processing of Personal Data by the Commission;
- a description of the categories of individuals and categories of Personal Data processed by the Commission;
- categories of recipients of Personal Data with whom the Commission shares Personal Data;
- where relevant, details of transfers to countries outwith the EU, including documentation of the transfer mechanism safeguards in place;
- details of how long the Commission keeps Personal Data in line with the Commission's Records Retention Policy;
- a description of technical and organisational security measures put in place to keep Personal Data secure; and
- the legitimate interest for the processing of Personal Data, if applicable.

The Commission will issue **transparency statements** from time to time to ensure that data subjects understand how their Personal Data is collected, used, stored, shared and deleted by the Commission.

We will take appropriate measures to provide information in **transparency statements** in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Commission's transparency statements are available on the Corporate website and Scotland on Tap website.

6. DATA PROTECTION FEE

All organisations that determine the purpose for which Personal Data is processed must pay a data protection fee unless they are exempt.

This is done by providing the ICO with certain information, including:

- the name and address of the Commission;
- the number of members of staff the Commission has;
- the turnover for the financial year;
- the name of the person completing the registration process; and
- the name of the Commission's Data Protection Officer.

As a public authority, the Commission's tier of registration is calculated with reference to staff numbers only and turnover is not considered. The Commission's Data Protection Officer is responsible for ensuring that the Commission pays the relevant data protection fee.

If any Commission employees believe that what they are going to do may be outside the scope of the Commission's current notification then they should contact their line manager. The line manager in turn should contact the Commission's Data Protection Officer to discuss if the notification needs to be updated.

7. ENFORCEMENT BY THE INFORMATION COMMISSIONER

The Information Commissioner has certain enforcement powers and may serve enforcement notices on an organisation where it considers that the Data Protection Principles have been breached. There are potential financial penalties and compensation payments due following on from a failure to comply with the DPL. In the unlikely event that you receive an enforcement notice or any other correspondence from the ICO, please refer this immediately to the Commission's Data Protection Officer.

8. COMPLIANCE AND REVIEW

The Commission considers this Policy to be extremely important. Any breach of the policy, or the Data Protection Principles, will be dealt with under our disciplinary procedures, which can be found in our Staff Handbook. In certain circumstances, a breach of this policy, or the Data Protection Principles, may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice.

The Commission will review this Policy and the associated procedures on a regular basis to ensure that they meet all legislative and regulatory requirements and best practice guidance. In addition, an annual audit and review of Personal Data held by the Commission will be carried out to ensure ongoing compliance with the provisions of the DPL.

Internal audit procedures will form an important part of establishing and sustaining good data protection practices. The Commission will review the Personal Data it processes and collects and assess this against the Data Protection Principles.

The Commission will undertake self-assessment to periodically check our compliance with the DPL; this Policy, regulatory and good practice guidance; and our working practices in the collection, processing and storage of Personal Data.

9. CHANGES TO PERSONAL DETAILS

It is in your own interest to keep your personal details up to date, so if you do change e.g. your name, address, or marital status, please follow the appropriate processes for updating personal information immediately. Fraudulent claims relating to personal details may result in disciplinary action and may lead to dismissal.