**Introduction**

The Commission is legally obliged to protect any personal information that we hold. This policy sets out how the Commission complies with the terms of the Data Protection Act 1998 and aims to ensure that the Commission fulfils the requirement for fair and lawful processing of personal data in the records which we create and receive during the course of our work.

## **Data Protection Act 1998**

The Commission is a data controller, as defined in section 1 (1) of the DPA and is obliged to ensure that all of the DPA requirements are implemented. As a public authority, the DPA applies to all personal data held by the Commission, both electronically and manually. There are eight data protection principles set out in the DPA which the Commission must comply with. These principles set out that data is:

* fairly and lawfully processed
* processed for limited purposes
* adequate, relevant and not excessive
* accurate and up to date
* not kept for longer than is necessary
* processed in line with individual’s rights
* secure
* not transferred to any countries outside the European Economic Area without adequate protection

## **Personal Data**

Section 1 of the Data Protection Act 1998 (DPA) defines personal data as *Information relating to a living individual who can be identified either from the data or from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.* As part of normal business operations, the Commission collects, holds and retains personal data about its employees, potential employees and stakeholders. Those whose personal data is held are known as data subjects.

The Commission ensures that personal data is collected and used fairly, is stored safely, and is managed in accordance with the data protection principles by ensuring that personal data is kept secure, accurate and up to date, and is securely disposed of at the appropriate time. Manual records containing personal data are stored securely in lockable cabinets and electronic records stored on the Commission’s shared drive are kept in restricted access folders. The Commission’s building meets the standards for accessing the GSI network. Access to the Commission’s computer network is controlled by individual user passwords. Passwords must meet specified security criteria. Access to personal data is based on a need to know basis.

**Sensitive Personal Data**

The DPA categorises some types of personal data as sensitive personal data. This includes data concerning racial or ethnic origin, political or religious beliefs, trade union membership, physical or mental health, sexual orientation and criminal records. With the exception of employee records, the majority of personal data held by the Commission is not sensitive. The Commission will not disclose personal data to any third party unlawfully.

**Processing of Personal Data During Recruitment and Selection**

Specific guidance on the processing and disposal of personal data obtained during any recruitment and selection process is also contained within the Commission’s Data Retention and Disposal policy and in the Records Disposal Procedure document.

* Sensitive data is requested via equal opportunities monitoring forms. These are kept separate from application forms and not disclosed to the shortlisting and interview panels.
* Only personal data that is relevant to the selection and potential on-going employment relationship is sought on application forms and similarly only personal data that is relevant to and necessary for the selection process is recorded and retained following interview.
* References are only taken up for candidates being offered a post and with the express consent of the individual.
* Application forms of successful candidates are retained on their personal file

**Right of Access**

An individual’s right to request their own personal data is known as a subject access request (SAR). The DPA gives individuals important rights, including the right to know what information is held about them and the right to correct information that is wrong. When recording information about individuals, the Commission should always use objective language. Staff should bear in mind that individuals may have a right to see what has been recorded if they request to do so.

Requests for personal data can be made by the data subject (the person whose personal data it is) or can be made by a third party on that person’s behalf, such as a parent on behalf of a child or a representative on behalf of an adult with incapacity. If a third party is making a request, reasonable checks should be taken to ensure that person has the authority to make the request. As a data controller, the Commission is required to respond to a SAR under the terms of the DPA. We have up to 40 calendar days to respond, from the data of receipt of the request (or from receipt of the further information to identify the requestor and to locate the requested data.

All staff have the right of access to personal data held on them by the Commission, with the exception of

* employment references, unless the referee has consented to disclosure or it is reasonable to do so without consent
* information provided in confidence by a third party

**Assessment**

If an individual believes there has been a breach of the DPA, they can request the Information Commissioners Office (ICO) to assess whether the Commission’s processing of personal data complies with the Act. The ICO can then ask the Commission to take steps to comply with the Act, issue enforcement notices and in extreme cases impose financial penalties in respect of deliberate or reckless handling of personal data which seriously breaches the DPA. Failure to comply with the data protection principles is not, on its own, a criminal offence.

**Staff Responsibilities**

The Chair of the Commission has overall responsibility for the Data Protection Policy. Responsibility is delegated to the Business Manager for ensuring that the policy and procedures for handling personal data are followed and that staff competence is maintained and developed.

All staff must follow the Commission’s data protection policy and procedures. Staff are encouraged to familiarise themselves with the implications of data protection in their job and the importance and legal obligation of keeping personal data secure. Relevant training opportunities can be provided to staff.

It is the responsibility of individual staff members to notify the Business Management Team of any changes in their personal data, such as home address, so that accurate records can be maintained, including for the information to be passed onto the appropriate contact, such as payroll and pension provider.

The Business Manager is responsible for ensuring that the Commission’s Data Protection Notification is kept up to date.

**Retention of Data**

The fifth data protection principle states that *personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.* The Commission’s Retention and Disposal Policy contains guidance on the retention and disposal of data held and created by the Commission and all staff must familiarise themselves with that policy.

**Protecting Personal Data**

During the course of their work at the Commission, all staff should be mindful about how they protect the personal data which they hold. The following practical tips are offered to assist staff;

* do not share or store passwords
* when creating passwords, use a strong password of at least 7 characters and which use a combination of lower and upper case letters, numbers and special keyboard characters
* consider whether the content of emails should be encrypted or password protected
* consider asking email recipients to acknowledge receipt of emails
* make sure you use the bcc field in emails if you do not want to reveal the names and email addresses of recipients
* be careful when using group email addresses
* dispose of any sensitive or confidential material in the confidential waste collection unit provided
* consider whether it is appropriate to leave a message on an answering machine, and if so only include necessary information
* do not send offensive emails about other people, their private lives or anything else that could potentially bring the Commission into disrepute
* be wary of people who may try and trick you into giving out personal details, trust your instincts
* do not believe emails that appear to come from your bank that ask for your account details or password
* do not open any attachments received in a spam email, delete the email
* do not send full credit card details as payment by email, as this may not be secure

Staff should also refer to the Commission’s Home Working Policy which provides detailed guidance on security procedures and best practice guidelines when working out of the office and how to keep information secure.

**Data Breaches**

In the event that a security breach of personal data (or a near miss) does occur, this must be reported immediately or as soon as is practically possible. The staff member concerned should report the incident to their line manager as soon as is practically possible and the Business Manager should also be informed. The Business Manager is responsible for recording all actions taken by the Commission to investigate and conclude the matter.

Information on the practical arrangements in response to data breaches can be found in the Commission’s Data Retention and Disposal policy.

**Additional Guidance**

The Information Commissioner’s Office is a useful resource to help organisations understand their obligations under the DPA and to keep them updated as when they change. Information and guidance on all areas of the DPA and the Commission’s responsibilities can be found on the ICO website at [www.ico.gov.uk](http://www.ico.gov.uk) and this should be the main point of reference.

Additionally, the ICO's office in Edinburgh provides a local point of contact for members of the public and organisations based in Scotland. As well as operating an advice service to address general enquiries, it promotes good practice in data protection by raising awareness of organisational responsibilities across all sectors. It also influences policy in related areas by working closely with the departments of the Scottish government and the wider public sector. The contact details are as follows:

The Information Commissioner's Office - Scotland
45 Melville Street
Edinburgh
EH3 7HL

Telephone: 0131 244 9001

Email: Scotland@ico.org.uk