Data Protection Policy:

The Scottish Parliament and SPCB is committed to protecting the rights of all individuals with regard to processing their personal data. This is carried out by complying with the requirements of:

- The Data Protection Act 1998 (the Act)
- Associated legislation and case law
- Best practice and guidance provided by the office of the UK Information Commissioner (ICO)
- The Scottish Parliament's notification with the UK Information Commissioner (ICO) which sets out the categories of personal data held by the parliament and the purposes for which they are held.
- The data protection framework developed and communicated by the Scottish Parliament

Data Protection Principles:

The Act requires that anyone processing personal data must comply with eight principles which represent best practice and which are legally enforceable. The principles require that information shall be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer than necessary
- Processed in line with the rights of individuals
- Kept secure
- Not transferred to other countries without adequate protection

The full text of these provisions is available here:

http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles

In order to meet the data protection principles the SPCB will:

- Fully observe the conditions regarding the fair collection and use of personal data.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process personal data only to the extent that it is required to fulfil operational purposes or to comply with legal requirements.
- Put in place adequate processes to ensure the quality of data.
- Hold personal data on our systems only for the length of time necessary to fulfil our operational purposes and in line with our corporate records retention schedule.
- Ensure the rights of the individuals about whom we hold data can be fully exercised (the right to be informed that processing is being undertaken, the right of subject access, the right to prevent processing in certain circumstances, the right to correct, rectify, block or erase information which is regarded as being incorrect).
- Take all appropriate technical and organisational security measures to safeguard personal data.
- Ensure that personal data held by the SPCB is not transferred to areas outside the EEA without appropriate safeguards.

In addition, the SPCB will ensure that:

- An individual within the organisation has specific responsibility for data protection.
- All SPCB staff and contractors managing and handling personal data are familiar with the data protection principles and understand that they must follow the data protection principles of good practice.
- This policy is available to each SPCB employee and complying with it is part of the terms and conditions of employment.
- Clear information about data protection requirements is available to all of our staff.
- Everyone managing and handling personal data is appropriately trained and supervised.

- Enquiries about handling personal data are promptly and courteously handled.
- Methods and performance of handling personal data are regularly assessed and evaluated.
- All MSPs and their staff are provided with guidance and best practice in handling personal data.
- The Head of Information Governance reports regularly to the Leadership Group which approves all changes to this policy.

Compliance

In order to operate effectively the Scottish Parliament must collect and use certain types of information including potentially sensitive personal data about individuals with whom it interacts. These may include for example current, past and prospective employees, MSPs and their staff, clients and customers, expert witnesses and advisers and others with whom it communicates. In addition it may be required to collect and use information in order to comply with the requirements of democratic processes.

All users of personal data held by the Scottish Parliament must comply with:

- The requirements of the Data Protection Act 1998
- All data protection guidance and codes of practice implemented by the office of the UK Information Commissioner(ICO)
- All data protection policy. guidance and processes implemented by the SPCB
- All associated information management and records management requirements including records retention best practice and information security requirements.

These requirements apply to all personal data held by the SPCB irrespective of format, where it is held, ownership, equipment or devices used.

Any breach of the parliament's policies, procedures or guidance in respect of processing personal data may result in the parliament being liable for the consequences and internal disciplinary action being taken.

Responsibilities

- The Head of Information Governance is responsible for day to day compliance with data protection requirements, developing guidance and providing advice and training

- All SPCB staff must undertake mandatory induction e-training on the requirements of the Data Protection Act
- All staff must undertake regular refresher e-training on the requirements of the Data Protection Act All staff have a responsibility to respect personal data and to maintain information security

Disclosure of personal data gathered during the course of your employment or assisting other to do so will be viewed by the SPCB with the utmost seriousness.

Information Security

All SPCB employees must comply with the guidance and standards set out in the Computer Security Policy and the Acceptable Use of IT Policy

http://www.scottish.parliament.uk/intranet/16251.aspx

http://www.scottish.parliament.uk/abouttheparliament/31563.aspx

Policy on managing the rights of data subjects

The Scottish Parliament is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

The right of subject access allows an individual to have access to the personal data held about them on either computer or manual files and to be supplied with a description (which will include the purposes for which it was processed and who it might be disclosed to) within 20 calendar days and where appropriate, to have it corrected or deleted. Individuals have a right to be:

- Told if their personal data is being processed
- Given a description of the personal data, the reasons why it is being processed and who it will be passed to
- Given a copy of the data
- Given details about the source of the data
- Given details about any automated decisions made on the basis of the data held

Individuals can see how the SPCB process personal data and can ask to see the information the SPCB holds about them by making a data protection subject access request here: http://www.parliament.scot/help/23315.aspx

Alternatively we will supply a leaflet which explains how to make a data protection subject access request.

All replies to SARs from the SPCB must provide

- An acknowledgement of receipt of the SAR
- A response within the statutory 40 calendar day deadline
- A response which makes all reasonable adjustments in line with the requirements of the requester
- All the relevant data
- A clear explanation for any data not included in the response
- An explanation of any technical or specialist terminology used

An SAR checklist must be completed for each SAR response *(a link to this will be provided here once the content of the guidance is agreed and published)*

All SAR responses must be completed using an SAR response template *(a link will be provided here to a template letter)*

Policy on management of data breaches

The Scottish Parliament is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

The Scottish Parliament undertakes to process personal data in a way that is safe and secure by taking all appropriate technical and other relevant measures against unauthorised or unlawful processing of data and against accidental loss, destruction and damage.

Should a data breach occur, the Scottish Parliament will invoke a data breach plan to:

- Contain the breach
- Make initial and ongoing assessments of risks
- Identify and notify affected stakeholders
- Notify the ICO of the breach
- Investigate the cause(s) of the breach
- Take corrective actions
- Regularly review new processes to ensure the breach is not repeated

The data breach plan will be invoked by a specialist team of experts to contain, manage and mitigate the risks to all data subjects who may be affected by the breach.

Policy on Data Sharing

The Scottish Parliament is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

In certain circumstances the SPCB may be asked to share personal data either routinely or on an individual "ad hoc" basis. In this context "sharing" means disclosing data from one or more organisations to an external third party or exchange of data between different parts of the same organisation including for example between the SPS and individual Members each of whom are individual data controllers.

The Scottish Parliament undertakes to ensure that the conditions for sharing personal data within the requirements of the Data Protection Act 1998 are t:

- the data subject consents to processing
- processing is necessary for the performance of a contract with the individual
- processing is required under a legal obligation
- processing is necessary to protect the vital interests of an individual
- processing is necessary to carry out a public function (for example administration of justice or statutory functions)
- processing is necessary in order to pursue the legitimate interests of the data controller or third parties

When third party data processors undertake processing on behalf of the SPCB, the SPCB will always t ensure in a written contract that:

- the processor only acts on instructions from the data controller
- the processor has adequate security in place either between internal offices or with other third party organisations and MSPs, SPCB staff must:
- Consider the appropriateness of sharing with the relative risks and consider appropriate options by completing a privacy impact assessment (PIA) on each type of data you plan to share using the approved PIA template

  http://www.parliament.scot/help/19154.aspx
- Complete, publish and communicate relevant privacy notices
- Complete and agree a data sharing agreement with each of the third parties or internal offices you plan to share data with
- Regularly review the content of the data sharing agreement

- Comply with the security requirements set out in the seventh Data Protection Principle and review regularly and in a way that is appropriate to the level of data being shared.
- Publish data sharing agreements on our website.
- Notify the ICO regarding new or ceased data sharing undertaken by the SPCB with any external third parties within 28 days.
- Note that information regarding data sharing may be requested under the Freedom of Information (Scotland) Act 2002.

For advice and guidance on data protection requirements contact:

The Head of Information Governance: claire.turnbull@parliament.scot