Guidance Title: Off Network Data Handling

Author: Alan Balharrie
Role: Head of Business IT & Broadcasting

Approved By:
Role:

Governance: Group
LG

Date: 25/01/2012
Version No: 0.1

Summary
As standard, all sensitive data should be processed and stored on the Parliament’s ICT network. However, there is an appreciation this may not always be practical or possible. This document provides guidance to SPCB staff, contractors, consultants and suppliers to may require to process sensitive data away from the Parliament’s network.

Objective
This document provides guidance to help ensure that all sensitive Parliamentary data transported or transferred beyond the Parliament’s ICT network, remains secure.

Audience
All SPCB staff, contractors, consultants and suppliers who have access to the Scottish Parliament’s information and associated assets are responsible for ensuring the security of that information and assets.

Exceptions
This guidance is not relevant to Members and their staff.

Policy
All sensitive data will, wherever practical, be processed and stored on the Parliament’s ICT network.

Where sensitive data has to be transferred and stored away from the Parliament network, the appropriate Office Head will ensure that the impact of the loss, or misuse of the data is considered, and that the risks of transferring the data from the network are accepted. In accepting the risks, the Office Head will ensure that all reasonable steps to safeguard the data are planned, documented and implemented.

The Business Information Technology Office has produced, and will maintain, the following data handling guidance, which should be used to help safeguard sensitive information.

Background
The majority of information processed by SPCB staff on the Parliament network would not be categorised as sensitive, and would be freely available through general publication or by request.

There is however a need to occasionally process or store sensitive data on the Parliament network and systems (e.g. personal details of staff, or time sensitive information such as
Loss or inappropriate disclosure of sensitive parliament data can occur, either through theft, negligence or malicious misuse. These risks are greatly reduced when the data is processed on the Parliament network, but it is recognised that on occasion it is necessary to transfer or store parliament data away from the network.

The policy and guidance outlined in this document does not set out to prevent remote or home working, but instead lays out measures to ensure that when you work on sensitive Parliamentary Data beyond the Parliament network, you do so only when necessary, and in a secure manner.

Staff and Office Heads are best placed to decide if data is sensitive but as a guide, data can be deemed sensitive if the loss of it may:

- Adversely risk the smooth running of our operations and services
- Damage our reputation
- Place individuals at risk
- Potentially breach confidentiality or affect anyone’s personal privacy

Although all SPCB staff are responsible for the secure processing of data, the policy for the transfer of data from the parliament network puts an additional responsibility on the Office Head to ensure that risks are considered, and mitigating actions are undertaken to keep data secure. Office Heads may delegate the approval role to line managers.

---

**Guidance**

The Business Information Technology Office is well placed to offer advice and guidance on data security matters. If staff and Office Heads require support and advice in order to meet their responsibilities, then they should contact the BIT Helpdesk on ext. 86100.

Wherever practical, all sensitive data should be processed and stored on the Parliament’s ICT network. This objective can be achieved when working remotely by using the Parliament’s remote access systems. However it should be noted that you will need a connection to the internet and appropriate software installed on the machine you are using.

Where offline processing of sensitive data is necessary, it is recommended that a Parliament laptop is used. Parliament laptops employ full hard disk encryption and password protection to help ensure that all data stored on the laptop is secure. The BIT Office operates a laptop loan pool and further information can be found here - [http://www.scottish.parliament.uk/intranet/25216.aspx](http://www.scottish.parliament.uk/intranet/25216.aspx).

Where it is necessary to transfer data on portable media (e.g. memory sticks, CDs, DVDs, etc.) it is important to take measures to protect the data. These measures will include ensuring the physical security of the portable media, as well as encrypting, or at very least password protecting the data. It is important to remember that data copied on to portable media will not automatically be encrypted and sensitive data should be deleted from the device as soon as possible.

Sensitive data should not be sent out-with the Parliament via email unless appropriate measures are taken to protect the data (encryption / password protection). BlackBerry
devices issued by the Parliament are password protected and encrypted by default. If you lose or mislay personal or sensitive data, you must report it immediately to your Head of Office.

Should Parliamentary supplied equipment be stolen or lost, please ensure you inform the Parliamentary Police Unit as soon as possible, and complete a Theft / Damage / Accounting Loss Report Form.

If you lose your BlackBerry device, please contact the IT Helpdesk on 0131 34 86100 or at IT Helpdesk immediately, and we will send a command to the device that will delete all data currently stored on it.

### Data Transfer Process
Please consider the steps outlined below before storing, transferring or removing data from processing away from the Parliament’s ICT Network:

1. **Is the data personal, sensitive or business critical?**
   - **Yes**: If you are sure that the data is not personal, sensitive or business critical, it can be removed from the Parliament network. It is however still advisable to follow the guidance from BiT on safe data handling.
   - **No**: Removing sensitive data from the Parliament network should only happen when absolutely necessary. Heads of Office should take all reasonable steps to ensure that staff are not required to remove.

2. **Is it necessary for the data to be transferred or stored off the parliament?**
   - **Yes**: Sensitive data should not be removed without first assessing, understanding and accepting the associated risks.
   - **No**: Sensitive data will not be removed without identifying all appropriate actions that need to be taken to mitigate the risks of removing the data. BiT have produced guidance on safe data handling and this should be consulted and followed.

3. **Have you and your Office Head assessed the nature and sensitivity of the data, including the impact if it is lost or misused, and accepted the risks?**
   - **Yes**: If the options to safeguard the data do not sufficiently mitigate the risks of removing the data to your Head of Office’s satisfaction and they are unwilling to give their approval, the data should not be removed from the Parliament network.
   - **No**: If you have and your Head of Office given their approval for removal of data from the Parliament network.

4. **Have you and your Head of Office planned and implemented all reasonable steps to safeguard the data?**
   - **Yes**: If the options to safeguard the data do not sufficiently mitigate the risks of removing the data to your Head of Office’s satisfaction and they are unwilling to give their approval, the data should not be removed from the Parliament network.
   - **No**: If you have and your Head of Office given their approval for removal of data from the Parliament network.

5. **Has your Head of Office given their approval for removal of data from the Parliament network?**
   - **Yes**: If you have and your Head of Office given their approval for removal of data from the Parliament network.
   - **No**: If the options to safeguard the data do not sufficiently mitigate the risks of removing the data to your Head of Office’s satisfaction and they are unwilling to give their approval, the data should not be removed from the Parliament network.

6. **Remove, process and return the data in accordance with your plan and as approved by your Head of Office.**