

Appendix 5

Information Management and Security

1.1 Everyone working with the Electoral Commission has a responsibility to protect sensitive and personal information at all times. This brief guide will provide you with some key measures to ensure that you are doing all you can to ensure Information is managed in a secure and responsible way. It will also point you in the direction of more detailed guidance, policies and support.

Protected Information

1.2 The Electoral Commission maintains three types of Information;

- **UNCLASSIFIED** – this would include information/records on the ‘X: drive’, accessible to all users. Most information falls into this category.
- **PERSONAL** – This information would contain identification details of an individual, such as name; age; gender; address; phone numbers; bank account details and; nationality. If disclosed without permission, they could cause distress or damage and breach the person’s privacy or human rights.
- **SENSITIVE** – This is information given in confidence that might result in embarrassment and loss if revealed to unauthorised parties. For example: “commercial in confidence”, “allegation casework” “enforcement actions” etc.

Data Protection

1.3 The Commission collects the personal information of a variety of individuals in the course of its business. As well as those who work for it, the Commission acquires personal data in a number of ways when it discharges its statutory functions, e.g. during an investigation into party’s receipt of donations, in the course of maintaining the electoral register, in receiving responses to boundary review consultations and when sending out and receiving information electronically.

1.4 Responsibilities when handling this type of information include:

- Personal information should be stored securely and only accessible to those who have a specific reason
- Personal information should not be shared within or outside of the Commission without explicit consent.
- Personal information should be destroyed in a secure way
- Personal information should not be kept any longer than necessary.

Storage

- All electronic information should be stored on the x: drive, (using your Citrix connection) in accordance with naming conventions and file structure.
- Where possible, avoid saving information to personal or non Commission PC's.
- Best practice is to store paper information should in folders, organised to facilitate finding information quickly.
- Personal and/or Sensitive information should be held securely in locked cabinets or secure electronic folders.
- When disposing information, personal and/or sensitive information in paper form should be securely destroyed, i.e. shredded or returned to the Commission for disposal. Information in electronic form should be permanently deleted.

Portable Devices, (Laptops, Blackberrys etc)

- Ensure that the equipment is not unattended for any period of time and locked away when you have finished using.
- If you have to leave a laptop unattended and switched on for a period of time, please ensure the machine is locked by simultaneously pressing the <Ctrl><Alt><Delete> keys and selecting 'Lock Computer' option from the menu.
- Take into account your surroundings when viewing information e.g. on a train where the screen may be overlooked.
- Unauthorised users (e.g. children, partners, etc), should be prevented from using the equipment.
- If attaching/detaching removable media to/from a laptop, such as external floppy drives or memory sticks ensure it is carried out carefully. Please follow the instructions from the IT Helpdesk. If you are in any doubt consult the IT Helpdesk team.
- Avoid taking portable equipment to social venues such as bars, restaurants and clubs.
- The Commission is completing a process of encryption for all laptops. If you are unsure if your laptop has the encryption software installed, please contact the IT Helpdesk.

Incident reporting

1.5 Staff should immediately report any incidents where they suspect that the confidentiality of Commission information or, the security of its IT systems has been compromised. Examples would include;

- Loss of information that was being transported from one location to another.
- Loss of computer equipment.
- Suspected access to an IT system by an unauthorised person.

- Infection of a system by a computer virus.

Such incidents should be reported to the IT helpdesk in the first instance.

1.6 For further information please see the Information Management guidance pages on the intranet

<http://intranet.electoralcommission.org.uk/teams/informationguidance.cfm>

Advice & Contacts

1.7 For any further advice on this guidance, please contact the Information Management Team.

1.8 For advice on IT systems/equipment, encryptions, or to report an incident please contact the IT Helpdesk.