The Electoral Commission

# 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 make sure that 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** – Most of the Commission's 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, when receiving and publishing political party Statements of Accounts 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 to view it
- Personal information should not be shared within or outside of the Commission without explicit consent

- Personal information should only be used for the purpose that it was collected
- Personal information should be destroyed in a secure way
- Personal information should not be kept any longer than necessary.

## Storage

- If saving electronic information it should be stored on the Commission's network which you can access through your virtual PC
- Information must not be saved to non-Commission PCs or sent to personal email addresses
- Best practice is to store paper information in folders, organised to facilitate finding information quickly
- Personal and/or Sensitive information should ideally be reviewed in electronic form negating the need to print off copies. If in hardcopy format it must be held securely in locked cabinets. When disposing of 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, (iPads, Laptops, Blackberrys etc)

- Ensure that the equipment is not unattended for any period of time and locked away when you have finished using it
- 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 hard drives or memory sticks, ensure that 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.

## 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;

- Information which has accidentally been sent to the wrong recipient
- 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.

## 2 Portable Equipment

2.1 You may be supplied with a Blackberry, laptop or other mobile device e.g. an iPad, for use on Commission business on a long or short term loan.

2.2 It is also possible use a personal mobile device to access your Commission email account, this service is available on request from the IT helpdesk and is subject to approval by the Head of ICT. This is currently restricted to Apple iPads and iPhones.

2.3 You should take all necessary steps to protect this equipment and any information stored on it from damage or theft and observe the following:

- Do not store personal or confidential information on portable devices.
- When using portable equipment outside EC premises, ensure that the equipment has the minimum amount of information stored on it and is not left unattended
- Avoid taking portable equipment to social venues such as bars, restaurants and clubs
- Portable equipment stored in the office should be locked away in a cabinet or desk drawer. If left in a car, it should be locked in the boot

2.4 If you decide to use a personal mobile device to access Commission information you must still abide by the security and usage controls as set out below:

- You must not attempt to disable or circumvent the encryption software loaded on your laptop.
- You must use minimum six digit PIN code on your iPhone or iPad
- If you lose a piece of equipment or suspect that the information on it has been compromised, you must immediately report this to the IT Help Desk.
- The Commission reserves the right to remotely wipe **any** device that has connected to a Commission email account in the event that it is lost, stolen or misused to protect any information that may reside on it.

## Advice & Contacts

For any further advice on this guidance, please contact the Information Management Team on 020 7271 0703/0554.

For advice on IT systems and equipment or to report an incident please contact the IT Helpdesk on 020 7271 0599.

The Electoral Commission

# iPad Conditions of use - declaration

I have read and agree to the conditions of use as set out in the '**Acceptable use of e-communications and IT facilities**' and **'iPad – Setup and acceptable use**' documents, and understand that any breach will be taken seriously.

……..
Signed

……
Full name (block capitals)

……..
Date

*Please sign and return to the Secretary to the Commission Board, Electoral Commission, 3 Bunhill Row, London EC1Y 8YZ*