Commission for
Victims and Survivors

Data Security – Securing Personal Data
(Based on NICS Guidance)

Here are the 10 key rules that all Commission staff must follow to ensure the security of personal data:

1. **Staff who use a portable device are personally responsible for its safekeeping and for the security of any information it contains.**

2. **Be very careful with sensitive and personal data.** Sensitive data are any documents or e-mails that are, or should be, marked 'Restricted' or 'Protect – Personal Data'. Be especially careful about files which contain large volumes of personal data – e.g. spreadsheets with lists of personal details which may identify or relate to a 3rd party.

3. **If you leave any computer switched on and unattended press Ctrl / Alt / Delete and select 'Lock Computer'.**

4. **Sensitive or personal data must not be stored on a laptop unless it is encrypted.** ECNI Staff will ensure Commission laptops are encrypted as part of the IT SLA.

5. **Sensitive or personal data must not be stored on mobile phones or on removable media.** Removable media include USB data drives, external hard drives, CDs, or multi-media data storage cards.

6. **During office hours, laptops must not be left unattended.**

7. **Outside office hours, laptops that are left in the office must be stored in a suitable locked cabinet.**

8. **Be very careful if you take your laptop or portable device out of the office.** Take special care in public, at airport security checks, in cars, in hotel rooms and at conferences or meetings.

9. **Encrypted laptops are secure, but you must still take great care of them.** First of all they are high-cost and valuable items, but also if they are lost or stolen there will be a perception that sensitive or personal data has been compromised.

10. **Exceptions to these rules can only be made in the most exceptional circumstances and then only if approved in writing by the Secretary to the Commission.**

What information should be classified as PROTECT PERSONAL DATA?

There is no definitive definition. The table below is the current Cabinet Office working definition.

One or more pieces of information which can be used with public domain information to identify an individual	**combined with**	**Information about that individual whose release is likely to cause harm or distress**
• Name • Address (home or business or both) • Postcode • Email • Telephone number(s) • Driving license number • Date of birth		• Sensitive personal data as defined by section 2 of the Data Protection Act, including records relating to the criminal justice system and group membership • DNA or fingerprints • Bank, financial or credit card details • National Insurance number • Tax, benefit or pension records • Health records • Employment record • School attendance or records • Material relating to social services including child protection and housing
or		

Any source of information about 1000 or more identifiable individuals, other than information from the public domain.