COMPUTER AND COMMUNICATION TECHNOLOGY

ETHICS, PRIVACY AND SECURITY

SECURITY THREATS IN ICT AND REMEDIES

Security threats:

1. Viruses corrupting your entire system
2. Someone breaking into your system and altering files
3. A hacker using your computer to attack others
4. Someone stealing your computer and accessing your personal information
5. Physical threats like theft, fire and flood
6. Hardware failure for example your computer's hard disk (which stores your files and data) corrupting or failing.

What you can do

- ***The*** most important thing you can do is **make regular backups** (– safe copies of all the files containing your important information and data).
- You should keep a recent copy of the backup off site (away from your office) in case disaster strikes (it *can* happen!). Store on site copies securely, preferably in a fire-proof safe.
- You should also check on a regular basis to make sure your backups work and you can safely restore your files.
- There are several options for backing up your files. The right option for your organisation will depend on several factors such as how often and how much data you need to backup.

Other things you should do include:

- Develop a Backup Strategy, **back up your important files regularly, check you can restore them, and store a copy of your backups off site** (just in case you missed this the first time we mentioned it!).

- Install antivirus software and **ensure it's updating regularly** – new viruses come out all the time.
- Make sure you regularly download security updates for your computer's operating system (e.g. Windows XP and other Windows versions) and other software. This can usually be set to happen automatically.
- Install a firewall to protect your computers and network from malicious attack.
- If you have a wireless network make sure you enable extra security features.
- Don't respond to "spam" (unsolicited emails). Many spam messages contain viruses or contain links to (very convincing) fake websites that try to steal sensitive information like credit card details.
- Make sure staff and volunteers are aware of the issues and receive appropriate training and induction to your systems.
- Have an ICT Acceptable Use Policy. This will make it clear to everyone in the organisation what they should and shouldn't be doing to help keep equipment secure and use it responsibly.
- Choose and use secure passwords on computers and networks, and change them regularly to prevent unauthorised access to your organisation's information..
- Store your ICT equipment securely (especially portable items such as laptops, cameras etc.) – don't forget to lock up!
- Security-mark your equipment – you might stand a chance of getting it back in the event of theft.
- Get insurance! Make sure you have adequate cover for replacing your equipment should the need arise.