

IT & Mobile Phone Policy

General Policy Statement

A clear and fair Information Technology Policy is needed to ensure the safe and legal use of the IT network at MCFB.

The policy is in place to:

- Ensure the confidentiality of any personal information concerning service users or staff stored on the system.
- Protect the organisation from any illegal or damaging actions, either knowingly or unknowingly.
- Minimise the risks of virus attack, compromise of network systems and services.
- Provide clear guidance on the acceptable use of computer equipment.

1. General Usage Policy

Every user has a responsibility when using the MCFB IT network and equipment to act legally and is expected to exercise good judgement regarding the reasonableness of personal use of any equipment, including computers and peripheral equipment such as printers and mobile phones.

For security and network maintenance purposes, authorised individuals may monitor equipment, systems and network traffic at any time.

- 1.1 Keep all passwords secure, do not share with anyone outside the organisation.
- 1.2 All PCs, laptops and workstations should be secured with a password protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the machine is unattended.
- 1.3 Because information contained on portable computers is especially vulnerable, special care should be taken when using any of the laptops.
- 1.4 Any e-mails sent from an MCFB account should contain a disclaimer stating that the opinions expressed are strictly those of the sender and not necessarily those of MCFB (this will be added automatically to any mail being sent through MCFB's server).
- 1.5 Users should exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses.
- 1.6 E-mails should not be sent to large numbers of recipients without prior permission from the Office Manager or IT support. When sending e-mails to large distribution lists the BCC function should always be used, ensuring that members of distribution lists are not visible on intercepted or wrongly addressed mail.
- 1.7 Personal web-browsing (including social networking sites & instant messaging) should be kept to lunch times and should always avoid sites that could affect the security of the IT network at MCFB.

- 1.8 Use of personal laptops is permitted on the MCFB wireless network, but users should be aware that any equipment brought into the office is not covered by the MCFB insurance policy.
- 1.9 MCFB does not hold any liability for the security of credit / debit card details entered on the MCFB system.
- 1.10 Any problems / issues relating to the IT system at MCFB should be reported using the 'Office Reporting' File kept in the Admin area. You should immediately inform the Office Manager (or Duty Senior in their absence) of any urgent concerns – including anti-virus expiry and connection problems. *N.B. when reporting issues relating to a particular machine, please identify which machine you are referring to by location or with laptops please note the serial number (usually found on the back.)*

2. Guidelines on Anti- Virus Protection

- 2.1 Do not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source.
- 2.2 Do not open any files attached to an e-mail unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through e-mail. Better be safe than sorry and confirm that they really sent it.
- 2.3 Do not open any files attached to an e-mail if the subject line is questionable or unexpected.
- 2.4 Delete chain e-mails and junk. Do not forward or reply to any of them. These types of e-mail are considered spam, which is unsolicited, intrusive mail that clogs up the system.
- 2.5 Do not download any files from strangers.
- 2.6 Exercise caution when downloading files from the Internet, ensure that the source is a legitimate and reputable one.
- 2.7 Non- essential files or programs should not be downloaded without prior permission from the Office Manager or IT Support.
- 2.8 Downloading any files from insecure websites and programs including MSN is not permitted.

3. Data Storage

- 3.1 No sensitive or personal information concerning service users or staff should be taken out of the office and should not be saved onto desktops / hard drives (on MCFB or personal equipment) or portable storage devices (memory sticks, discs etc.) *Any information of this nature should be saved on the shared (Z:) drive in the relevant folder.*
- 3.2 Always back up important files on the shared drive.
- 3.3 All students should save work into their personal folder on the shared (Z:) drive and should delete the folder and its contents on their last day in the office. *Any documents relating to cases that will remain relevant after the student has left MCFB should be discussed with their practice teacher and decided where best to save the file on the MCFB system.*
- 3.4 Service users telephone numbers should not be stored on mobile phones (personal or belonging to MCFB).

Becky Robertson – Office Manager
16/03/10

Approved by Board 18/05/10