Business Services Organisation

BSO USE OF ICT EQUIPMENT

(version 1.0)

Approved at BSO Board on 25th February 2010

CONTENT

1. PURPOSE

1.1 This Use of ICT Equipment Policy outlines the permissible use of the HSC supplied ICT equipment.

1.2 This policy applies to **all staff**, including regular full-time, regular part-time, contractors, consultants, agency and temporary employees.

2. PROTECTION OF EQUIPMENT

2.1 Passwords

2.1.1 Passwords should not be shared with anyone including a line manager or ICT staff.

2.1.2 Passwords should always be changed immediately on suspicion of any compromise. The longer a password remains unchanged, the more opportunity a potential intruder will have to discover it. Any such incidents must be reported to the HSC ICT Security Manager.

2.1.3 The use of software for 'password-cracking' or any other means of discovering passwords is forbidden.

2.1.4 Screens, keyboards and printers should be physically positioned such that they are protected against accidental disclosure of passwords or any other confidential or sensitive data.

2.1.5 Staff should follow the following basic security password principles:-

- **YOUR PASSWORD MUST BE KEPT CONFIDENTIAL**;
- Do NOT write down your password;
    - Where it is necessary to write down a password (as, for example, a contingency measure) it should be stored in a sealed envelope in a safe. Access to the envelope in the safe should be restricted to contingency requirements only. Inspection of the envelope should be carried out on a regular basis by the officer to whom the password belongs and a record maintained.
    - Where electronic vaults[1] are used to store a number of passwords, the password used to access them must at least conform to the HSC minimum standard of 8 characters, 3 out of 4 character groups and be changed every 90 days.
- Do NOT reveal a password in an email message;
- Do NOT talk about a password in front of others;
- Do NOT hint at the format of a password;
- Do NOT reveal a password on questionnaires or security forms;

[1] Examples of these are KeePass Password Safe and Password Keeper (Blackberry).

- Do NOT share a password with family members;
- Do NOT reveal a password to a colleague before you go on leave;

- It should contain at least one character from each of the following four groups:-

    - Uppercase letters (A, B, C …)
    - Lowercase letters (a, b, c …)
    - Numerals (0, 1, 2, 3 …)
    - Symbols, meaning all characters not defined as letters or numerals (including ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).

2.1.6 Some Recommended password generation techniques are

- **Creating an Acronym from a Phrase**
  This is a common password technique that can really go a long way in helping you remember your password. For example:-
    - Chose the first two letters from each word. "Today the Weather is Sunny" creates 'Tothweissu'
    - Chose the first letter from each word, replacing the letter E with the number 3. "The Journey To The End Of The East Bay" creates Tjtt3ot3b
    - Chose the first letter from each word as well as using numbers and special characters to complete the password. "My mother's birthday is 05-28. When is yours?" creates Mmbi05-28.Wiy?

- **Misspell Common Words**
  Most commonly you can use this technique to spell word phonetically, however any misspelling that you can remember will suffice. For example:-
    - Telephone0 could be Tellyfone0

- **Combining Words/Dates By Alternating Characters**

  This method uses two or more words and dates and alternates them every other character. For example:

    - "Twist & shout" would be "Tswhiosutt&"
    - "Paul@2010" would be "P2a0u10@"

2.1.7 When creating a password avoid the following as their use makes it easier for someone to work your password out either by guessing or using a password cracking too:-

- ***Avoid using basic personal information***. This can include:

    - Names of family members, close friends, or pets
    - Birthdays, Anniversaries, Dates Of Birth

    - National Insurance Numbers, Pin Numbers, Account Numbers
    - Current Or Previous Addresses, Phone Number
    - Car make, model and registration

- ***Avoid using you any portion of your Username***. Variations of the Username are the first things generic password hacking software will attempt.
- ***Avoid sequences***. Ensure that you do not use 'abcdefg' or '123456′. Also be weary of keyboard sequences, such as 'qwerty' or 'asdf1234′ or even shapes like 'rfvbnhyt'.
- ***Avoid keeping default passwords***. This is important because identity thieves can often find out how popular sites generate their random passwords (or at least the format). It's essential to change these as quickly as possible.
- ***Avoid complete words, especially common ones*** - The most basic password hacking software often checks databases of common dictionary words (even in foreign languages). No, spelling words backwards does not get around this, either.

2.1.8 Automated log-on procedures may contain passwords but should themselves be protected. For example, log-on procedures performed by striking a single function key should request the input of the password. If a macro or similar device is used to automate log-on then the user should be required to enter the password in order to activate the macro.

2.2 Patching & Anti-virus updates

2.2.1 Staff must allow security and functionality software updates to deploy when connected to the network where it does not impact on critical patient care. Otherwise this should be at the next earliest convenience.

2.2.2 Staff assigned PCs that are not regularly attached to the network must make special arrangements to have security patches and anti-virus software updated at least every 2 months.

2.3 Secure Storage / Protection of Equipment

2.3.1 Portable computers including laptops, PDAs, tablets, etc. must be stored in locked furniture when left unattended.

2.3.2 PCs left unattended at anytime must be at least locked using the Windows Lock Computer facility (Windows Logo Key+L). Alternatively use Ctrl-Alt-Delete and then Enter.

2.3.3 Where a PC is used by multiple users, during planned absences which exceed 2 hours or out of office hours, it must be logged out of the Network.

3. PROTECTION OF DATA

3.1 Staff should be aware that even with password-protected screensavers and boot-up passwords it is not possible to wholly guard against information on local hard disks being accessed by unauthorised users.

3.2 Therefore no sensitive data may be stored on PCs unless protected by encryption software this is approved by the BSO-ITS.

3.3 All BSO laptops will have encryption software e.g. PGP, Bitlocker or Becrypt installed and can therefore be removed from official premises.

3.4 Where patient identifiable/sensitive information is to be processed or held outside official premises, BSO-ITS approved encryption MUST be applied when in transit or at rest. This includes the use of removable media[2].

3.5 There are no automatic backup procedures in place for information stored locally on PC hard disks (this includes laptops) and data should only be stored temporarily on them when not connected to the network. Staff must ensure it is backed up on a network folder.

3.6 Staff should particularly be careful if changing the standard default set-up for their word-processing, spreadsheet, etc. software. Where staff use their local hard disk as the primary storage area for data it is recommended that software configurations be set to use their network account for storing the backup files.

3.7 If in doubt about the level of encryption required please contact the HSC ICT Security Manager.

4. SOFTWARE

4.1 Installation of new software or hardware, or changes to configurations, are only permitted provided appropriate licensing arrangements or other similar conditions of the supplier are met (see also the Use of the Internet Policy, in regard to downloading software).

4.2 Staff should note that disabling security software (such as anti-virus or application control programs) on HSC equipment is strictly forbidden.

4.3 Only officially provided and approved software must be loaded onto computers. This includes software for the visually impaired. This should only be installed by ICT staff, authorised HSC staff, or contracted ICT staff. All software present on HSC systems or equipment must be business related. The HSC has a legal obligation to ensure that no unlicensed software is present on its computers. If found it should be removed immediately. This includes but is not limited to:-

- Games;

[2] Removable media includes but is not limited to USD data pens, optical discs (Blu-ray, DVD, CD), memory cards, floppy/zip disks, magnetic tape and external hard disk drives.

- P2P file sharing tools;
- Internet based instant messaging applications;
- personal mobile phone software;
- portable media device software;
- proxy avoidance tools.

4.4 Only business related videos or audio files are permitted to be stored on HSC equipment including file servers.

5. PERSONAL DEVICES

5.1 Staff **MUST NOT** attach and/or install personal hardware devices to HSC ICT equipment. These include but are not limited to:-

- USB data pens;
- portable media players eg ipods.
- portable hard drives;
- mobile / smart phones;
- Personal Digital Assistants;
- digital cameras;
- Modems.

5.2 Staff must not connect personal computing equipment such as laptops or desktops to the HSC network. If there is a business requirement to do so, staff should contact the HSC ICT Security Manager where the request will be evaluated.

5.3 One exception to this is the use of a home PC to access the SSL Remote Access Service. This is subjected to a number of security checks (anti-virus, firewall and operating system) before a connection to the HSC network is permitted. In this case no documents can be saved or printed locally. Further information on the SSL VPN service is available from the HSC Security website - http://hpssweb.n-i.nhs.uk/security/website/Secure_Access/Secure_Access.html

6. MOBILE DEVICES

6.1 No sensitive data **MUST** be stored on mobile devices such as mobile phones, smart devices or blackberries unless protected by BSO-ITS approved encryption software.

6.2 Users of mobile devices such as smart phones or blackberries should inform the HSC ICT Security Manager immediately if the device is stolen or lost. This is to ensure that all steps are taken to remotely disable the device and the appropriate people notified.

7. MOBILE WORKING

7.1 Use of Equipment

7.1.1 If an officially provided PC is used outside secure official premises, it should be used only by an authorised member of staff. The PC must not be connected to any unauthorised external networks and must not use removable media that has not been officially approved and supplied.

7.1.2 Any PC that may previously have been connected to the Internet other than through the local network, for example through a standalone ADSL or a third party contractor, must not subsequently be attached to the local network without approval of the HSC ICT Security Manager. All laptops that access the Internet via the HSC "Checkpoint VPN" remote access service are exempt from this check as their internet access is controlled by BSO-ITS security systems.

7.1.3 Staff carrying or using a PC off the organisation's premises must take all reasonable steps to guard against their theft, loss or damage, and against unauthorised use.

7.1.4 Such equipment may not be used for any other purpose and must not be used by any person other than the nominated member of staff.

7.2 Guidelines for Health and Safety

7.2.1 Staff with remote access should be aware of their health and safety responsibilities and ensure that their home insurance policy covers home working.

8. INCIDENT REPORTING

8.1 Any actual or suspected security incident must be directly reported to the HSC ICT Security Manager. Naturally, theft or loss of HSC equipment should be reported but cases involving theft or loss of non-HSC equipment that contained any class of HSC material must also be reported without delay.

8.2 The following web site is to be used to record security incidents
http://hpssweb.n-i.nhs.uk/security/website/Feedback/Security-Incident-Form.html
More details are available from the web site.

8.3 Staff should be aware that all losses of ICT equipment or sensitive data are investigated and reported to the Health Minister.

8.4 Staff that fail to report security incidents that have an adverse impact on HSC services, its reputation or any data that it holds may be subject to disciplinary procedures.

9. LEAVERS AND CHANGE OF EMPLOYMENT

9.1 Users should delete any personal information such as emails and documents from the PC or personal file shares on the network when leaving the organisation.

9.2 HSC employees are required to return all HSC equipment once their employment is terminated. This includes but is not limited to;

- PC hardware (inc. laptops);
- USB data pens
- mobile phones;
- smart phones eg. Blackberrys;
- digital cameras;
- authentication tokens;
- PDAs;
- portal hard drives;
- CD and DVD ROMS containing licensed software or HSC specific data;
- printers;
- floppy disks.

9.3 All ID and access cards MUST be returned to your line manager.

9.4 Line managers and Human Resources are required to contact BSO-ITS as soon as possible with the name of employee, department and leaving date to enable access to email, HSC networks and other computer systems to be removed.

9.5 Staff are reminded that HSC equipment is allocated on a per post basis not on a per person basis. Therefore BSO-ITS and your line manager will review the equipment allocated to you when you move post.

10. MONITORING

10.1 Staff should note that, as is permitted by legislation, the HSC ICT Security Manager and deputy in the BSO-ITS will monitor and review internet activity and analyse usage patterns. Use will be routinely monitored from time to time, and may be specifically monitored at any time when this is deemed necessary for compliance or other reasons, including the prevention or detection of illegal activities.

10.2 Users of HSC ICT resources, including Internet and e-mail facilities, should be aware, and must accept as a condition of use, that their usage of such facilities will be monitored and may be reviewed whether use is for the conduct of official business or for personal use.

11. NON–COMPLIANCE

11.1 Any breach of this policy can result in disciplinary action which may result in dismissal.

11.2 Non-compliance can also damage the reputation of the HSC and open the HSC and the individual to a host of legal liabilities

12. LIABILITY

12.1 Staff should be aware that they might be personally liable to prosecution and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim by a person that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.