COMPUTER AND DATA SECURITY PROCEDURE (inc. REQUEST TO WORK FROM HOME)

Introduction

The purpose of this procedure is to define the arrangements and responsibilities for the physical security of computer hardware, backup of computer data, verification that the backups are effective, and storage of backup data. It also sets out the basis on which software additions may be made to individual PCs, the system or the network.

It is essential that the practice has full and accessible data backups to ensure that data can be restored in the event of any system failure, meaning normal operations can be resumed quickly and effectively.

There are also a number of precautions to be taken to protect the physical security of computers. These precautions depend on the situation. Different precautions need to be taken for computers used away from the workplace and for laptops used in a variety of locations.

In view of the accidental releases of personal data from a variety of Government organisations it is generally recognised that the risk involved in transporting data “off site” is far greater than the risk of accidental destruction or loss whilst the information is on the premises:

- Patient identifiable information is secure
- Data transfer methods are secure
- That remedial action is being taken if these two issues are weak

In addition:

- Personal identifiable information is not to be stored on removable devices such as CDs, memory-sticks and external hard-drives etc. unless it is encrypted
- Data is not to be downloaded or stored on portable media such as laptops, mobile phones, PDAs etc. unless it is encrypted
- Personal identifiable information is not to be stored on PC equipment in non-secure areas unless it is encrypted.

These requirements apply to all public sector organisations.

Given the complexity of adequate encryption tools, the above requirements will be enforced within the practice pending further instructions.

STORAGE AND BACKUP

Any data stored on a computer hard drive is vulnerable to the following:

- Loss due to a computer virus.
- Physical loss or damage of the computer, for example:

    - Theft
    - Water damage
    - Fire or physical destruction
    - Faulty components
    - Software

In particular, there is a risk of breach of confidentiality where a computer is stolen or otherwise falls into unauthorised hands.

The following precautions should be taken:

- Servers should not be used as regular workstations for any application
- Access to servers will be authorised and all server access will be recorded in a dedicated logbook – a locked security system will be used to protect the server
- Use a shared drive on a networked server for all data wherever possible
- A documented procedure for daily backup of the server will be maintained and a full backup will be taken every working day
- Backups will be stored in a fireproof data safe
- No patient data will be stored on a PC or other equipment in non-secure areas
- Use a reputable backup validation service at regular, pre-programmed intervals
- Have a five-tape system ensuring that, even if the back-up procedure fails, the loss of data is reduced
- Take extra precautions to protect the server. Servers should be sited away from risk of accidental knocking, spillage of drinks, leaking pipes, overheating due to radiators and be inaccessible to the public
- Where a PC is standalone, ensure that the hard drive is backed up regularly and any confidential data is password protected

  The Senior Administrator will be responsible for daily monitoring of the back-up and for the security of tapes.

  In the event of the absence of the nominated person the Deputy Practice Manager will assume responsibility for this procedure.

  Five backup tapes are available labelled Monday – Friday and should be used in rotation. The tapes should be renewed every six months.

  Each morning The Senior Administrator will check the backup routine event log:

    - Open backup job monitoring on screen
    - Check that the event log for the previous night (shown by date) shows 100% with no errors. If any failure is reported, contact the IT support desk on **01234 581850**
    - Record the date, tape used, tape use count and status and sign the **back-up tape log** (see appendix 1) located in Admin Room 1
    - Place the new tape in the tape streamer
    - Place the most recent tape in the data safe

Specified non-clinical data will be backed up monthly.

In the event that clinical data restoration is required, contact the IT support desk on 01234 581850 for guidance before proceeding further.

In the event of non-clinical restoration of data contact ITS 01234 581850

Every three months, or at the interval recommended by the clinical supplier, a clinical backup tape is to be delivered off-site to the clinical system supplier who will verify that the tape contains a valid and restorable backup.

BULK DATA EXTRACTIONS

No bulk extracts or manipulation of data or coding is permitted other than with the prior permission of the Practice & Business Manager.

DATA SAFE

Backup tapes will be stored in a data safe tested to European Standard EN1047-1. A standard fire-proof safe designed for paper records will not be used, as these give inadequate heat protection for tape media which must be kept below 52 degrees C.

The data safe will be anchored into position and will be sited in an area less likely to be subject to flooding or other hazards.

PROTECTION AGAINST VIRUSES

Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from CDROM/DVDROM, other storage media and by direct links via e-mail and web browsing.

The following precautions will be taken:

- Virus protection software will be installed on ALL computer equipment
- There will be a documented procedure for anti-virus software version control and update
- Automatic or pre-programmed updates will be used wherever possible
- A clear procedure via nominated staff will deal with any viruses found
- Software installation will be in accordance with this protocol and only authorised licensed software is to be installed on the organisation's equipment
- The Computer, Internet and Email Policy [*] will contain specific instructions on downloads, attachments and unknown senders etc.
- Ensure that preview panes in email software are not open when sending/receiving mail
- Physical restrictions e.g. drive locks / disable drives will be used where appropriate
- All staff will be made aware of data security issues in all IT-related protocols and procedures
- Data security will be mentioned in the practice's disciplinary policy

INSTALLATION OF SOFTWARE

Software purchases will be authorised by the Practice & Business Manager who will supervise the loading of the software onto the system or individual PCs in accordance with the software licence.

Staff are prohibited from installing or upgrading personal or purchased software without the written permission of the nominated person.

Staff are prohibited from downloading software, upgrades or add-ins from the internet without the written permission of the nominated person.

Staff are permitted to receive and open files received in the normal course of business providing they have been received and virus scanned through the standard virus software installed by the clinical system supplier.

HARDWARE

Staff and contractors are not permitted to introduce or otherwise use any hardware or removable storage devices into the practice other than that which has been provided, or pre-approved, by the practice.

The Practice & Business Manager is responsible for ensuring that the practice has adequate supplies of removable storage media of a type approved for use in the practice. The use of removable storage media is by authorised staff only.

Removable storage media (including CDs and other similar temporary items) which are no longer required must be stored securely for destruction along with other PC equipment. The Practice & Business Manager will be responsible for the secure storage of these items.

PROTECTION AGAINST PHYSICAL HAZARDS

WATER

- Check that the PC or server are not at risk of pipes and radiators which, if damaged, could allow water onto the equipment
- Do not place PCs near to taps/ sinks
- Do not place PCs close to windows subject to condensation and water collection on windowsills
- Ensure that the PC is not kept in a damp or steamy environment

FIRE AND HEAT

- Computers generate quite a bit of heat and should be used in a well-ventilated environment. Overheating can cause malfunction, as well as creating a fire hazard
- Try to place the PC away from direct sunlight and as far as possible from radiators or other sources of heat
- Normal health and safety protection of the building against fire, such as smoke alarms and CO_2 fire extinguishers should be sufficient for computers. If backup tapes are kept on the premises they must be protected against fire in a fireproof safe
- Have the wiring and plugs checked annually
- Ensure that ventilators on computers are kept clear

- Do not stack paper on or near computers

ENVIRONMENTAL HAZARDS

Computers are vulnerable to malfunction due to poor air quality, dust, smoke, humidity and grease. A normal working environment should not affect safe running of the computer, but if any of the above are present consider having an air filter. Ensure that the environment is generally clean and free from dust.

POWER SUPPLY

Protect against power surges by having an uninterrupted power supply fitted to the server.

In the event of the premises becoming unusable, a pre-tested 'IT disaster recovery procedure' needs to ensure that systems can be run off site, including replacement hardware.

PROTECTION AGAINST THEFT OR VANDALISM VIA ACCESS TO THE BUILDING

In addition, the following precautions should be considered to protect the building, such as:

- Burglar alarm with intruder monitor in each room
- Locks on all downstairs windows
- Appropriate locks or keypad access only, on all doors
- Seal off separate areas of the building e.g. reception area should have shutters and a lockable door and all separate rooms should be locked when the building is unoccupied
- Where the building is not fully occupied e.g. during out of hours clinics, only the required rooms and corridors should be accessible to the public e.g. administration areas and consulting rooms not in use to be kept locked
- Ensure there is a clear responsibility for locking the doors and securing the building when unoccupied
- Ensure any keys stored on site are not in an obvious place and any instructions regarding key locations or keypad codes are not easily accessible
- Have a procedure for dealing with unauthorised access during opening hours
- Ensure keypad codes and alarm codes are changed regularly (monthly) especially after staff leave employment
- Ensure that there is appropriate insurance cover where applicable
- Use bolt-down security server cages
- Do not store patient identifiable information on PC equipment which is not contained in a secure area
- Maintain a separate record of hardware and software specifications of every PC in the building
- Specific precautions relating to IT hardware are:
    - Use security locks to fix IT hardware to desks to prevent easy removal
    - Locate PCs as far away from windows as possible
    - Clearly 'security mark' all PCs and all parts of PCs i.e. screen, monitor, keypad.
    - Have an asset register for all computer equipment, which includes serial numbers
    - Ensure every PC is password protected

MOBILE COMPUTING

Particular precautions need to be taken with portable devices, both when they are used on site and when taken offsite.

On-site
Laptops, palmtops and any other portable devices are more vulnerable than PCs, because they are easier to pick up and remove and therefore more desirable to the opportunist thief. It is also less likely, in some circumstances, that their loss will be noticed immediately. However, because of their size, it is possible to provide extra protection:

- When the device is not in use, it should be stored in a secure location
- Where it is left on the premises overnight, it should be stored in a locked cupboard or drawer
- Where the device is shared, have a mechanism for recording who is responsible for it at any particular time
- Patient or personal identifiable information should not be contained on laptops or other portable devices or removable storage devices
- Password protection

IN TRANSIT

Computers should not be left unattended in cars. Where this is unavoidable, ensure that the car is locked and the computer is out of site in the boot or at least covered up if there is not a boot.

The responsible staff member should take the device with them if leaving the vehicle for any length of time.

USE IN A PUBLIC PLACE

- The device should remain with the member of staff at all times
- Care should be taken when using the device that confidential data cannot be overlooked by members of the public e.g. on public transport

USE IN A PATIENT'S HOME

- The device should have a password protected screen saver
- The device should remain with the member of staff at all times
- Care should be taken that confidential data cannot be seen by other members of the family / carers

USE ON OTHER PREMISES (E.G. OUTREACH CLINIC)

- The device should remain with the member of staff at all times
- When the device is not in use it should be stored in a secure location
- Where it is left on the premises overnight, it should be stored in a locked cupboard or drawer

SMART CARDS

Where access to the clinical or other systems is to be controlled via the issue of a smart card the following will apply:

- Smart cards are issued to an individual on a named basis and are for the use of that person only
- The access level relating to an individual is personal and must not be shared or otherwise made accessible to another member of staff
- The smart card is to be kept under the personal control of the individual to whom it has been issued at all times and must not be left inserted into a smart card reader when the individual is not present
- The smart card will normally be held on a neck cord or other similar device to ensure that it remains with the owner
- On leaving a terminal the smart card is to be removed ***on every occasion***
- Staff members are not to leave their cards on the premises when they leave work
- Staff members leaving their cards at home will be required to go and collect them
- Staff members sharing smart cards on more than one occasion will be considered for disciplinary action in accordance with the practice's normal procedures. This would normally be after an informal warning
- Staff members must report the loss of a card to [*insert name*] as soon as it is known that the card is missing
- Smart cards will not normally be handed over between individuals. In the event of a staff member needing to relinquish a card (e.g. over a holiday period) then this will be passed back to the practice manager or nominated person who will log the transfer and retain the card securely

HOME WORKING

OVERVIEW

In some instances it may be appropriate for a member of staff to work at home. Careful consideration needs to be given to the following issues:

- Will the member of staff have dial-in access to the practice's systems?
- Will the member of staff be using the confidential data for work purposes or for the individual's own purposes (coursework, research etc)?
- Does the staff member require separate registration under the Data Protection Act?

Under no circumstances will patient or personal identifiable information be permitted to be removed from the premises in any format without the express permission of the data controller. Work at home is anticipated to relate to administration or non-personal information only.

Home Workers will be made fully aware of their Information Governance responsibilities. Appropriate forms must be completed to ensure that users understand the terms and conditions for the use of the media in question.

Assurances will also be sought when taking confidential information away from the practice in paper format. Home workers must ensure that such information will be kept secure and inaccessible to other family members or visitors to the household.

A log sheet will be used to identify individual items being taken out of and being returned to the practice.

EMPLOYEE'S OWN PC WITHOUT DIAL-IN ACCESS

The following should be considered:

- Consider the physical security of the PC – vulnerability to theft or unauthorised access. Computer equipment should never be left unattended when logged in and switched on. Computer equipment must be kept in a secure place when not in use
- Care should be taken that confidential data cannot be overseen or accessed by unauthorised third parties including other members of the family / visitors to the employee's home
- Risk of loss of the data due to viruses, accidental loss etc. Ensure that up-to-date virus protection is in place and updated regularly
- The device should have a password-protected screen saver
- Back-up of essential data
- Disposal of printouts of confidential data generated at the employee's home
- Ensuring the data is fully deleted from the computer after use
- Ensuring the employee does not use the data for any purpose other than for that authorised
- If the work is ongoing, ensuring that the data is destroyed when the employee leaves employment or replaces their home computer
- If data is backed up using disks or USB sticks these must be password protected and stored in a secure place – any such data backup copies are to be transported securely

EMPLOYEE'S OWN PC WITH DIAL- IN ACCESS

The following should be considered:

- Remote access to practice systems should be previously authorised by The Practice & Business Manager
- Other family members or visitors to the employee's home who use the computer must never have access to confidential data
- The device should have a password-protected screen saver
- Consider the physical security of the PC – vulnerability to theft or unauthorised access. Computer equipment should never be left unattended when logged in and switched on. Computer equipment must be kept in a secure place when not in use
- Ensure that up-to-date virus protection is in place and updated regularly
- Care should be taken that confidential data cannot be overseen by unauthorised third parties including other members of the family / visitors to the employee's home
- Ensure that strong authentication is in place
- Ensure that data is not held on the computer hard drive
- If data is to be backed up using disks or USB sticks, these must be password protected and stored in a secure place – any such data backup copies are to be transported securely
- Ensure that other modems are not attached to the computer, as this invalidates the organisations "code of connection" and places the system's security at risk
- Emailing confidential data to or from a remote PC should only be undertaken when adequate protection is in place
- Ensure proper disposal of printouts of confidential data generated at the employee's home

USING AN NHS ORGANISATION'S COMPUTER

- Remote access to practice systems should be previously authorised by The Practice & Business Manager
- Other family members or visitors to the employee's home who use the computer must never have access to confidential data
- The device should have a password-protected screen saver
- Consider the physical security of the PC – vulnerability to theft or unauthorised access. Computer equipment should never be left unattended when logged in and switched on. Computer equipment must be kept in a secure place when not in use
- Ensure that up-to-date virus protection is in place and updated regularly
- Care should be taken that confidential data cannot be overseen by unauthorised third parties including other members of the family / visitors to the employee's home
- Ensure that other modems are not attached to the computer, as this invalidates the organisation's "code of connection" and places the system at risk
- Ensure proper disposal of printouts of confidential data generated at the employee's home
- Ensure the employee does not use the data for any purpose other than that authorised
- Ensure that no data is held on the computer hard drive where the employee has dial-in access

THE PRACTICE'S RESPONSIBILITIES

The practice must ensure that the employee fully understands all their responsibilities with regard to confidential data. The employee must sign a written statement of the responsibilities they are undertaking towards the security of the data.

The practice must ensure that there are arrangements to clear employees' hard drives of any confidential data as soon as this becomes appropriate.

The practice must ensure that arrangements are in place for the confidential disposal of any paper waste generated at the employees' home.

The practice must maintain an up-to-date record of any data being processed / accessed at an employee's home and the purpose for which the employee is accessing the data. It is the employee's responsibility to use the data for the purpose intended and no other and they must be absolutely clear as to what that purpose is.

The practice must be clear as to when it is passing ownership of data to an individual (e.g. for project work or, research and development) and this should be authorised by the Caldicott Guardian / Data Controller. The individual may then need to be separately registered under the Data Protection Act 1998.

RESOURCES

Server Tape backup procedure **[*]**
Mobile Phone Policy **[*]**

Employees who wish to apply to work from home should complete the form Request for authorisation to work from home – shown below:

Request for authorisation to work from home

This form should be completed and submitted to (practice manager/Caldicott Guardian)

Name _____

Position _____

Practice _____

Describe the data you intend to work on at home. Indicate the patient identifiers you will hold and any sensitive information such as clinical details.

Explain why the work needs to be carried out away from the workplace.

Please indicate whether you will be working on your own computer or one provided by your employer.

What arrangements have been made to dispose of any paper printouts generated which hold person identifiable data.

I have read, understood and accept the terms of the practice's computer and data security procedure.

Signed: **Date:**
(employee)

Authorised by:

Signed: **Date:**
(manager)

Print Name: **Position:**

DR KHOKHER & PARTNERS

APPENDIX 1 - TAPE BACK-UP SCHEDULE Sheet 1

If the backup routine fails and there is no obvious cause (e.g. no tape in drive) contact the Senior Administrator

Day	Date	Scheduled Tape	Actual Tape (+Reason for change)	Successful? Yes / No	If no, reason (if known) and details of action taken	Checked by
Mon		Monday				
Tues		Tuesday				
Wed		Wednesday				
Thur		Thursday				
Fri		FRIDAY				
Mon		Monday				
Tue		Tuesday				
Wed		Wednesday				
Thur		Thursday				
Fri		FRIDAY				
Mon		Monday				
Tue		Tuesday				
Wed		Wednesday				
Thur		Thursday				
Fri		FRIDAY				