Crown House Surgery

Computer & Data Security Procedure & Remote Working

Version Number	**Author**	**Date**
1	JM	31.1.2022

INTRODUCTION

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

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

Data over than that held within the clinical system is held on a Windows Server 2016 Virtual Machine hosted by an ESX hypervisor on Dell T330 Server hardware. Personal data is held in individual named folders mapped individually to each named user as a home drive; shared data is held in a shared folder accessible to practice staff only.

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 – this information is held by the building management, CHP
- Use a shared drive on a networked server for all data wherever possible
- The practice's IT support is responsible for the procedure for daily backups of the server & full backups, a copy of these logs can be obtained by contacting the IT helpdesk.
- No patient data will be stored on a PC or other equipment in non-secure areas
- 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
- For immediate recovery of files and folders, Shadow Copies are enabled on the site server allowing recovery through the Previous Versions feature.

In the event that clinical or non clinical data restoration is required, contact the IT support desk on 0114 3051030 for guidance.

USE OF ONLINE CONSULTATION/VIDEO-CONFERENCING SOFTWARE (INC. MS TEAMS)

Video sharing/conferencing apps such as Skype, Whatsapp, AccuRx or Microsoft Teams can be used for private 1:1 chats and group chats without the need to create a team. Any instant messages (IMs) received by a user whilst offline will be available next time that user goes online.

Conversation history and chats remain, even after closing the application. Users must not share sensitive information within a chat unless it is intended for all invited participants. Invited participants will be able to read the chat even if they do not join the meeting, or if they have already been disconnected. Use a separate email or Teams chat for private conversations amongst a sub-group of colleagues.

To ensure we keep Personal Confidential Data (PCD) secure however, we need your assistance so that Teams is used correctly, both safely and securely. Therefore you MUST adhere to the following:

MINIMISE THE USE OF PCD (PERSONAL CONFIDENTIAL DATA).

- Only send PCD via instant message where absolutely necessary, use NHSMail to NHSMail (nhs.net) in the first instance.
- If it is essential to send PCD via Teams, then it must only be sent in an encrypted and password protected attachment from a CCG device.
- However, PCD can be safely verbally disclosed during video and voice conferences, but
- PCD should NOT be openly used if the Teams meeting is being recorded

IF YOU CHOOSE TO ACCESS ON PERSONAL DEVICES THEN ENSURE THE DEVICE MEETS THE FOLLOWING CRITERIA

- Device is encrypted
- Device is fully security updated (Patched)
- Device requires authentication (i.e. 6 Digit PIN, Complex Password, Fingerprint, FaceID)

BULK DATA EXTRACTIONS

No bulk extracts or manipulation of data or coding is permitted other than with the prior permission of Dr Michael Bazlinton, Information Governance Lead.

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 will be followed via instruction from the IT helpdesk 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 Dr Michael Bazlinton, Information Governance Officer. Jennifer Mimms, Practice Business & Quality Manager 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 permission of the Jennifer Mimms.

Staff are prohibited from downloading software, upgrades or add-ins from the internet without the permission of Jennifer Mimms.

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.

Jennifer Mimms 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. Jennifer Mimms 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/Laptops near to taps/ sinks
- Do not place PCs/Laptops close to windows subject to condensation and water collection on windowsills
- Ensure that the PC/Laptop 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/Laptop 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
- Have the wiring and plugs checked annually
- Ensure that ventilators on PCs/Laptops are kept clear
- Do not stack paper on or near PCs/Laptops

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

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
- Smart Cards must not be kept in the computer either overnight or when the room is not being used
- Locks on all downstairs windows
- Appropriate locks or keypad access only, on all doors
- All patient area rooms should be locked when not in use even if it is for just a few minutes.
- 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 laptops to desks to prevent easy removal
    - Locate PCs/Laptops as far away from windows as possible
    - 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 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, drawer or secured with a laptop cable lock
- 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, drawer or secured with a laptop cable lock

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 to ensure smart cards are left overnight in a secure/locked drawer/cabinet or taken home with them & stored responsibly
- 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 disciplinary procedure. This would normally be after an informal warning
- Staff members must report the loss of a card to Jennifer Mimms 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, Business & Quality 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.

USING AN NHS ORGANISATION'S COMPUTER

- Remote access to practice systems should be previously authorised by Jennifer Mimms
- Other family members or visitors to the employee's home are not permitted to use the computer nor 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
- Headphones must be worn when making & receiving phone calls through the laptop, via Surgery Connect, when other members of the household or visitors to the household are present
- Calls should must not be made or received when other members of the household or visitors to the household are present in the same room

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.

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 Business & Quality 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.

NHS Laptop, with secure VPN connection

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:**

Print Name: Jennifer Mimms **Position:** Practice Business & Quality Manager