VENTURE
Health Group

Policy Title	**Information Governance Policy**
Policy Number	**17**
Version	**0.11**
Date Ratified	**04/10/2023**
Primary Author	**Satish Maddineni**
Responsible Committee	**Board of Directors**
Review Date	**04/10/2025**
Target Audience	**All staff & Directors**

Table of Contents

Purpose

This Policy **defines the responsibilities for information governance within the Venture Health Group (Venture), the steps to be taken to guard against risks, and the action to be taken in the event of a breach of security**.

This Policy applies to all staff with access to Company data and / or information systems, and to all types of data (paper-based and electronic) and information systems.

Venture is an insourcing organisation providing consultant delivered clinical services to NHS trusts on NHS properties (host organisations). Venture works closely with host organisations and ensures mutually agreed complete alignment of all information governance processes at the start of all new contracted clinical services.

Policy objectives

1. To ensure that information (including the information about patients and other types of confidential information) are:
   - held securely
   - obtained fairly and lawfully
   - recorded and managed in an accurate and reliable manner
   - used in an effective and ethical way.
   - shared and disclosed in an appropriate and lawful manner

2. To provide assurance to all staff members that the data they use:
   - is available and can always be accessed.
   - has integrity and has not been deliberately or inadvertently modified from an approved version.
   - is kept confidential (i.e., sensitive information is only available to those persons authorised to have access)
   - can be produced to comply with legitimate requests from law enforcement agencies, from data subjects as defined by the *Data Protection Act 2018 and General Data Protection Regulations 2016 (GDPR)*, and in any other circumstances for which there is current or future legal provision.

3. To ensure protection against risks, including but not limited to:
   - loss or damage to Company finance, personnel, and service user records.
   - damage to reputations caused by breaches of security.
   - liability for the consequences of breaches of security.

4. To provide appropriate staff training in the awareness of the need for security, the measures taken to achieve this, and the consequences of security breaches. Additional specialist training will be provided to staff members who have responsibility for the IT systems.

Responsibilities

- **The Information Governance and Digital Lead**, Mr James Broome, who also acts as the Data Protection Lead and is the Senior Risk Information Manager (& is a Director) **will retain overall responsibility for overseeing the implementation of this Information Governance Policy**. In particular this will include ensuring that appropriate security measures are in place for centrally provided IT systems, the IT infrastructure systems and the Company-wide management information systems.
- **The Information Governance and Digital Lead will liaise closely with the Registered Manager**, Mr Satish Maddineni on all related activities.
- As Venture is a medical insourcing organisation, it does not hold any patient data on its own IT systems. All patient level data is held securely within the host organisation that Venture is providing clinical services within.
- The host organisation is contractually responsible for ensuring that appropriate security is in place to protect data and information systems under their control and for acting when appropriate. This will focus upon physical security for access to rooms, filing cabinets and computers. Systems and procedures are in place to protect the security of both paper-based and computer-based information and the mechanisms for responding and assisting in investigations in the event of a security breach.
- All staff with access to information must take all precautions to protect data held within Venture, to adhere to the principles of the *Data Protection Act 2018 and General Data Protection regulations (GDPR) 2016*, to ensure that confidentiality of data is respected and to comply with any guidelines that may be issued by Venture.

The Information Governance and Digital Lead will carry out an annual audit or risk assessment on all information for which Venture is responsible and take action to ensure that security measures are in place that are up-to-date and consistent with the risk assessment. The risk assessment will focus upon the physical security of equipment, systems security, access to data, and Disaster Recovery Plans.

Handling breaches of IT security

The risks associated with using IT systems connected to the Internet are considerable. Breaches of security affecting electronic information include the following situations:

- loss of data.
- inadvertent release of data to unauthorised persons.
- unauthorised access to one or more information systems which may affect the security of the system itself.

Any person suspecting a breach of IT security should report the matter immediately to the Information Governance and Digital Lead, or the Governance Lead or the Board of Directors.

Where a breach of security is confirmed, the Board of Directors will undertake a full investigation. A full report on the actions taken, lessons learned and an action plan for improvements will be issued for staff awareness.

Following successful remedy of a breach the Board of Directors will delegate a named staff member to take responsibility to actively monitor Venture's IT network and periodically probe for security breaches and weaknesses within permissible limits, and to report their findings to the Board of Directors.

CQC identifies the following additional policies under the scope of Information governance:

- GDPR Policy
- Computer and Data Security Procedure
- Freedom of Information

GDPR Policy

Introduction

The Data Protection Act 2018 (DPA) requires a clear direction on policy for **security of information held within an organisation** and provides individuals with a right of access to a copy of information held about them. **As of May 2018, this policy is now referred to as the General Data Protection Regulation (GDPR).**

Venture needs to collect personal information about people with whom it deals to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts.

The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law.

No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the **Data Protection Act 2018.**

The lawful and proper treatment of personal information by Venture is extremely important to the success of our business and to maintain the confidence of our service users and employees. We ensure that Venture treats personal information lawfully and correctly.

This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

The Access to Medical Records policy covers Subject Access Requests under the Data Protection Act.

General Data Protection Regulation Principles

We support fully and comply with the eight principles of the Act which are summarised below: **fair & lawful; purposes; adequacy; accuracy; retention; rights; security and international transfers**

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained/processed for specific lawful purposes.

3. Personal data held must be adequate, relevant and not excessive.

4. Personal data must be accurate and kept up to date.

5. Personal data shall not be kept for longer than necessary.

6. Personal data shall be processed in accordance with rights of data subjects.

7. Personal data must be kept secure.

8. Personal data should not be transferred to other countries without the same levels of data protection (e.g. outside the EEA)

Who does the GDPR apply to?

The GDPR applies to 'controllers' **and** 'processors.

A controller determines the purposes and means of processing personal data.

A processor is responsible for processing personal data on behalf of a controller.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

The GDPR applies to processing carried out by private clinics operating within the EU. It also applies to private clinics outside the EU that offer goods or services to individuals in the EU.

The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

The UK's DPA 2018 has already enacted the EU GDPR's requirements into UK law, and with effect from 1 January 2021, the DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)) Regulations 2019 amended the DPA 2018 and merged it with the requirements of the EU GDPR to form a new, UK specific data protection regime that works in a UK context after Brexit as part of the DPA 2018.
This new regime is known as 'the UK GDPR'.

UK organisations need to amend their GDPR documentation to align it with the requirements of the UK GDPR. Article 30 records, privacy notices, DPIAs (data protection impact assessments), DSARs (data subject access requests) and documentation covering international data flows must all reflect the UK's independent jurisdiction and the specific scope and wording of the UK GDPR.

Any UK organisation that offers goods or services to, or monitors the behaviour of, EU residents will also have to comply with the EU GDPR and will reflect this in its process documentation.

What information does the GDPR apply to?

Personal data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way private clinics collect information about people.
The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data"
The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing

Staff Responsibilities

All staff will, through appropriate training and responsible management:

- comply at all times with the above General Data Protection Regulation principles
- observe all forms of guidance and procedures about the collection and use of personal information
- understand fully the purposes for which Venture uses personal information
- collect and process appropriate information, and only in accordance with the purposes for which it is to be used by Venture to meet its service needs or legal requirements
- ensure the information is correctly inputted into Venture's systems
- ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required

- on receipt of a request from an individual for information held about them by or on behalf of immediately notify the Registered Manager

- not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian / Information Governance Lead

- understand that breaches of this Policy may result in disciplinary action, including dismissal

Venture's Responsibilities

Venture works closely with the host organisation in which it is providing clinical services. Therefore, there is mirroring of information governance and GDPR processes between the two organisations. Within this context, Venture will:

- Ensure that there is always one person with overall responsibility for data protection. Currently this person is Mr James Broome (the Information Governance and Digital Lead, and Director). Any questions about data protection should, in the first instance, be directed to him. In his absence, the Registered Manager (Mr Satish Maddineni) will take on these responsibilities.

- Maintain its registration with the Information Commissioner's Office

- Ensure that all subject access requests are dealt with as per our Access to Medical Records policy

- Provide training for all staff members who handle personal information

- Provide clear lines of report and supervision for compliance with data protection and also have a system for breach reporting

- Carry out regular checks to monitor and assess new processing of personal data and to ensure Venture notification to the Information Commissioner is updated to take account of any changes in processing of personal data

- Develop and maintain DPA procedures to include: roles and responsibilities, notification, subject access, training and compliance testing

- Display a Privacy Notice on the website explaining to patients Venture's policy (see below) plus a copy of the Information Commissioners certificate.

- Liaise with the host organisation so that patients are clearly aware of how to access their medical records via the host organisation or via Venture. Venture also houses a leaflet "Access to Medical Records" [*] for the information of patients on its website. Venture also displays the certificate of registration with the Information Commissioners office.

- Take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's consent, unless otherwise legally compliant. This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.

- Undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.

- Maintain a system of "Significant Event Reporting" through a no-blame culture to capture and address incidents which threaten compliance.

- Ensure confidentiality clauses are included in all contracts of employment.

- Ensure that all aspects of confidentiality and information security are promoted to all staff.

- Remain committed to the security of patient and staff records.

- Ensure that any personal staff data requested by public or government bodies such as HMRC i.e. age, sexual orientation and religion etc., is not released without the written consent of the staff member

Statement

The recording of data within Venture is under the management and control of Mr James Broome who is the Information Governance and Digital Lead, the data protection lead and the Senior Information Risk Officer.

The quality of data, the use of templates and the use of specific coding is reviewed on an ongoing basis and the findings are discussed at clinical policy meetings.

The Information Governance and Digital Lead is responsible for data quality issues within Venture and will ensure accuracy and consistency in recording data among both the doctors and administrative staff.

Mr Satish Maddineni is the Registered Manager responsible for audit and exception identification and reporting within Venture and will work closely with the Information Governance and Digital Lead

Any queries should be addressed to the lead Doctor.

Signed:

James Broome
Information Governance Lead

Date: 21st May 2023

Satish Maddineni
Registered Manager

Date: 21st May 2023

Appendix A: Patient Poster on Data Protection

DATA PROTECTION ACT – PATIENT INFORMATION

We need to hold personal information about you on our computer systems and occasionally in paper records to help us to look after your health needs. Your Venture clinician is responsible for their accuracy and safe keeping. Please help to keep your record up to date by informing Venture and the NHS organisation where your treatment has been delivered of any changes to your circumstances.

Doctors and staff have access to your medical records to enable them to do their jobs. From time to time, information may be shared with others involved in your care if it is necessary. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other circumstances you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you. Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

You have a right to see your records if you wish.

Appendix B: Computer and Data Security Procedure

Introduction

Venture is an insourcing organisation providing consultant delivered clinical services to NHS trusts on NHS properties (host organisations). Venture works closely with host organisations and ensures mutually agreed complete alignment of all information governance processes at the start of all new contracted clinical services. Venture does not hold any patient data on its IT systems. All patient related data is held on the host organisations IT systems.

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. The host organisation is responsible for all hardware and its security. Venture staff are responsible for complying with all IT governance procedures.

It is essential that Venture 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. For clinical notes, this is officiated in alliance with The Northern Care Alliance (the host organisation).

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. The host organisation is responsible for the protection of all IT hardware used to provide clinical services by Venture staff.

In view of the accidental releases of personal data from a variety of Government private clinics 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 private healthcare organisations.

Given the complexity of adequate encryption tools, the above requirements will be enforced within Venture 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 including
    - Theft
    - Water damage
    - Fire or physical destruction
    - Faulty components
    - Software

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 Information Governance and Digital Lead will be responsible for the monitoring of the back-up and for the security of storage arrangements of Venture. This responsibility is shared with the host organisation Information Governance team and the Digital Security Network.

All laptops and workstations are automatically backed-up by the host organisation in an active fashion in a real-time manner via the digital processes embedded on all digital devices that link to the host providers intranet and all electronic patient records.

All digital equipment used by Venture in the management of all host providers patients have been provided by the host provider and are compliant with these robust and secure processes. This model is employed by Venture whenever it provides clinical services to any host organisation.

The host organisation IT team ensure review of the backup routine event log and share any concerns with Venture**.** The review is as follows:

- 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, the IT review team launch a deep dive

Specified non-clinical data is backed up by Venture in a real time fashion on secure servers. All clinical data or patient centric data is actively managed by the Northern Care Alliance IT teams (host organisation) through trust-wide IT governance processes.

In the event that clinical data restoration is required, contact the host provider IT support desk.

In the event of non-clinical restoration of data contact Information Governance and Digital Lead – info@venturehealth.co.uk or the Registered Manager – governance@venturehealth.co.uk

All clinical data is backed up actively in real-time by the host organisation. All clinical data handled by Venture staff is on laptops or workstations provided by the host organisation on trust property that are compliant with the IT governance framework and procedures of the host trust.

Bulk Data Extractions

No bulk extracts or manipulation of data or coding is permitted other than with the prior permission of the IT governance team of the Northern Care Alliance and Venture.

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. All data safe issues are owned by the host organisation – the Northern Care Alliance.

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 host organisation has an extensive IT infrastructure with robust standard operating procedures for this. All clinical data is handled by Venture staff on host organisation IT equipment only. This principal is mirrored with all new host organisations.

There is a suite of robust and extensive precautions that are taken by the host organisation – the following precautions are a few examples:

- 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 private clinic'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 private clinic's disciplinary policy

Installation Of Software

Software purchases must be authorised by the Information Governance and Digital Lead who will supervise the loading of the software onto the Venture system or individual PCs in accordance with the software licence.

New software cannot be loaded onto the host organisation IT equipment or systems without express administrator permission from the IT department.

Staff are prohibited from installing or upgrading personal or purchased software on any Venture equipment.

Staff are prohibited from downloading software, upgrades, or add-ins from the internet on any Venture equipment.

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 Venture other than that which has been provided, or pre-approved, by Venture.

The Information Governance and Digital Lead is responsible for ensuring that Venture has adequate supplies of removable storage media of a type approved for use in the clinical arena. 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. Venture 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

(Undertaken In Conjunction with the Host Organisation {Northern Care Alliance})

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

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
- 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

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 clinic'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 private clinic 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.

Staff's own PC without dial-in access

Venture does not support staff utilising personal computer equipment for any Venture services.

In the unlikely scenario where this is the case 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

Venture does not support staff utilising personal computer equipment for any Venture services.

In the unlikely scenario where this is the case the following should be considered:

- Remote access to clinic systems should be previously authorised by a Venture Director
- 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 private clinics "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 The Host Organisation's computer

- Remote access to clinic systems should be previously authorised by a Venture Director
- 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 private clinic'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

Venture's Responsibilities:

Venture must ensure that all staff fully understand their responsibilities regarding confidential data. Staff must sign a written statement at the commencement of employment by Venture of the responsibilities they are undertaking towards the security of the data.

Venture must ensure that there are arrangements to clear staff's hard drives of any confidential data as soon as this becomes appropriate.

Venture must ensure that arrangements are in place for the confidential disposal of any paper waste generated at staff's homes.

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

Venture 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 GDPR & Data Protection Act 2018.

Appendix C: Freedom of Information Policy

FREEDOM OF INFORMATION POLICY

INTRODUCTION

The following policy sets out the approach to the freedom of information (foi) act 2000 by a service.

POLICY

- The service will comply with the FOI Act and sees it as an opportunity to enhance public trust and confidence in the service
- The service will maintain a comprehensive 'Publication Scheme' that provides information which is readily accessible without the need for a formal FoI Act request
- According to The Freedom of Information Act 2000, it is required for Trusts to respond to requests within **20 working days** and the Information Commissioner's Office (ICO) has set a statutory timescale for public authorities to achieve 90% of all requests to be responded. Venture will fully comply to these regulations
- However, if necessary we will extend this timescale to give full consideration to a public interest test. If we do not expect to meet the deadline, we will inform the requester as soon as possible of the reasons for the delay and when we expect to have made a decision
- The service will continue to protect the personal data entrusted to us, by disclosing it only in accordance with the GDPR and Data Protection Act 2018
- The service will provide advice and assistance to requesters to facilitate their use of FoI Act. We will publish our procedures and assist requesters to clarify their requests so that they can obtain the information that they require
- The service will work with **Manchester Council** and other bodies with whom we work to ensure that we can meet our FoI Act obligations, including the disclosure of any information that they hold on our behalf
- The service will apply the exemptions provided in the FoI Act and, where qualified exemptions exist, the service will disclose the information unless the balance of public interest lies in withholding it
- The service will consult with third parties before disclosing information that could affect their rights and interests. However, according to the FoI Act, the service must take the final decision on disclosure
- The service will charge for information requests in line with the FoI Act fees regulations or other applicable regulations, including GDPR & Data Protection Act 2018
- The service will record all FoI Act requests and our responses and will monitor our performance in handling requests and complaints
- The service will ensure that all staff are aware of their obligations under FoI Act and will include FoI Act education in the induction of all new staff

Information to be published	**How the information can be obtained** (eg hard copy, website)	**Cost**
Class1 - Who we are and what we do (Organisational information, structures, locations and contacts) This will be current information only		
Healthcare Professionals in the service		
Contact details for the service (named contacts where possible with telephone number and email address (if used))		
Opening hours		
Other staffing details		
Class 2 – What we spend and how we spend it (Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit) Current and previous financial year as a minimum		
Total cost to the LHB/HSSB of our contracted services.		
Audit of income		
Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews) Current and previous year as a minimum		
Plans for the development and provision of clinical services		
Class 4 – How we make decisions (Decision making processes and records of decisions) Current and previous year as a minimum		
Records of decisions made in the service affecting the provision of clinical services		
Class 5 – Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities) Current information only (mark “not held” against any policies not actually held)		

Policies and procedures about the employment of staff		
Internal instructions to staff and policies relating to the delivery of services		
Equality and diversity policy		
Health and safety policy		
Complaints procedures (including those covering requests for information and operating the publication scheme)		
Records management policies (records retention, destruction and archive)		
Data protection policies		
Policies and procedures for handling requests for information		
Patients' charter		
Class 6 – Lists and Registers Currently maintained lists and registers only		
Any publicly available register or list (if any are held this should be publicised; in most circumstances existing access provisions will suffice)		
Class 7 – The services we offer (Information about the services we offer, including leaflets, guidance and newsletters produced for the public) Current information only		
Charges for any of these services		
Information leaflets		
Out of hours arrangements		

http://www.legislation.gov.uk/ukpga/2000/36/contents