<Company Name>

Computer Usage Policy

I have read and understood the policy:

Print Name…………………..

Signature……………………

Dated………………………...

Index

1. Overview

Introduction

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards. All records should meet legal and regulatory compliance and professional practice recommendations.

Organisations need to have policies and procedures in place that ensure records are created, managed, handled and stored securely. <company name> endeavours to have such policies and procedures that adhere to the HORUS model:

- **Holding** information securely and confidentially
- **Obtaining** information fairly and efficiently
- **Recording** information accurately and reliably
- **Using** information effectively and ethically
- **Sharing** information appropriately and lawfully

In committing to these, <company name> will ensure that anyone processing personal data in relation to the organisation will comply with the eight enforceable principles of good practice as indicated in the Data Protection Act 1998:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than necessary
6. Processed in accordance with the data subject's rights
7. Secure
8. Not transferred to countries without adequate protection

We will ensure that:

- Records are created, maintained and stored to standards which meet legal and regulatory compliance and professional practice recommendations; and
- Customers can be assured of appropriately completed records and that all information is managed within the regulated body to ensure confidentiality. Information will be made available on how to access records and issues governing consent.

Everyone needs to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

The principle behind this code is that no-one shall misuse any information or allow others to.

This policy has been written to meet the following legal requirements and best practice Guidance:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000

2. Records

Information Asset Register
<company name> maintains and Information Asset Register that identifies all types of patient and staff data this is retained and identifies how it is kept secure.

Customer Information
Identifiable customer information is only recorded only where:

- Necessary for the delivery of high quality service from <company name>
- Record retention is a regulatory requirement.

Staff Information
Staff information is retained for HR purposes in both paper and electronic form.

3. Data Protection

Data Security
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 e.g. 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.

Precautions to be taken include:

- Servers should not be used as regular workstations for any application.
- Access to servers should be authorised by senior personnel.
- A full backup must be taken every working day.
- At least 2 revolving backups with a copy taken off site at least weekly.
- 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.
- All computers are to be completely shut down at the end of the working day
- All users are allocated a system security level appropriate to their needs
- Where a PC is standalone, ensure that important data on the hard drive is backed up regularly and any confidential data is password protected.

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

Precautions to be taken include:

- Ensure virus protection software is installed on ALL computer equipment.
- Anyone discovering a virus must report this to the CEO
- All software must be purchased, installed and configured by the specialist Outsourced Provider. This includes all software packages, software upgrades and add-ons – however minor. It also includes shareware, freeware and any items downloaded from the internet.

- No document or file from any source outside the organisation can be used unless it has been scanned for viruses using the virus scanning software.
- Staff should treat email attachments that they are not expecting with extreme caution – it does not matter if the sender is known to you. Viruses are often sent this way. If unsure what an attachment is for, or why someone has sent it, this should not be opened.
- Staff should note that intentionally introducing files which cause computer problems could result in prosecution under the Computer Misuse Act 1990.
- Staff must not violate licence agreements by making illegal copies of software. It is not permissible to download software from the internet or install from CD or disc without prior authorisation. Software licensing will be arranged and recorded as part of the procurement and/or installation process. Any unlicensed software found on a practice PC must be deleted or disabled.

Installation of Software
Software purchases will be authorised by the CEO and the specialist Outsourced Provider 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 permission.

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

Internet and Email Use
All staff must use the Internet and email in a responsible manner. Inappropriate use may be subject to disciplinary or legal action.

Protection against Physical Hazards
Staff must be aware of and comply with the following:

- Water
  - Ensure that the PC or server is 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 / 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 CO2 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. Inspect your system visually and have the unit cleaned by a professional to reduce risk of failure or damage.
- Power Supply - Protect against power surges by having an uninterrupted power supply fitted to the server.

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 the building.
- Appropriate locks or keypad access only, on all doors.
- 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.
- Ensure that there is appropriate insurance cover where applicable.
- Maintain a separate record of hardware specifications of every PC in the office
- Specific precautions relating to IT hardware are:
  - Locate PCs as far away from windows as possible.
  - Clearly ‘security mark’ all PCs and all parts of PCs i.e. screen, monitor, keyboard.
  - Have an asset register for all computer equipment, which includes serial numbers.
  - Ensure every PC is password protected.
  - Have important laptops and PCs encrypted.

Mobile Computing
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.

Computers should not be left unattended in cars. Where this is unavoidable, ensure that the car is locked and the computer is out of sight in the boot or at least covered up if there isn’t a boot. The responsible staff member should take the device with them if leaving the vehicle for any length of time.

Where a device is being used in a Public Place it should remain with the member of staff at all times, and care should be taken to ensure that confidential data cannot be overlooked by members of the public, e.g. on public transport.

Confidentiality

Any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information.

4. IT equipment

<company name> outsources its IT requirements to a specialist provider who provides hardware, software, technical support and strategic IT advice.

Hardware
Specialist advice is taken with regard to all hardware purchases.

Software
Specialist advice is taken with regard to all software purchases.

Antivirus software is updated according to advice from technical support but this is generally more than once per year.

Technical support
Specialist support is retained to ensure smooth operation of systems including remote support and emergency support for both hardware and software.

User training
Staff are required to develop good IT skills and are used to working with information systems, business and office packages as required by their job roles

Disaster recovery
A business impact assessment and business continuity plans are undertaken/reviewed whenever there is a structural change in the IT infrastructure, including replacement of servers.

Daily back-ups combined with technical support that can provide a fully-configured replacement server within 48 hours comprise the key components of a disaster recovery plan.

5. Access Control Policy

System security comprises the following:

Risk Assessments
The system security requirements
Prior to implementation of strategic systems changes, a risk assessment will be undertaken to determine the security requirements given the data concerned. For example, the level and type of access controls, location of hardware associated with the system, type of data held, etc.

User Account Management
User accounts should be amended immediately upon there being a change in the staff team to ensure that all user accounts are appropriate. This could be the existence of an account of the level of information to which the member of staff has access and includes creation and removal of access rights.

The Chief Executive is responsible for ensuring that access rights are appropriate

Network Security
<company name> ensures that its local network is protected by authentication, encryption and network connection controls which prevent unauthorised access including via wireless technology.

Secure Logon Procedures

All computer systems should have a logon procedure that includes at least a unique user ID and password. The following features should be put in place for all <company name> systems:

- System/application identifiers are not to be displayed until the logon procedure has been successfully completed.
- Where login errors are made there should be no indication as to which part of logon information is incorrect. This prevents unauthorised users identifying patterns when attempting to gain access to systems.
- The number of unsuccessful consecutive logon attempts is limited to 3.
- There is no limit as to the maximum time allowed for any one logon. However, password protected screen savers are used prevent unauthorised use.
- The password being entered is not displayed in clear text. The systems show a number of asterisk characters.
- Passwords should not be transmitted in clear text over the network under any circumstances.

Identifying users

In order to facilitate access control and audit functions all users have unique identifiers in the form of a unique username and password combination. Group IDs are not to be used.

Password management system

A password management system should operate as follows:

- No group passwords on the system; all users will be identified as individuals (including system administrators) when they log on.
- Users should change their initial password (issued by the system administrator) following their first logon.
- The system should log user passwords and prevent re-use.
- Users should change their own passwords at least quarterly but can do so more often where they feel their current one has been compromised.
- There are to be no restrictions on the use of alphas and/or numerics in order that users can set memorable passwords and are therefore encouraged to change them frequently.
- Passwords should be stored separately from application system data.
- Passwords stored and transmitted in encrypted or hashed form? All passwords should be stored or transmitted using encryption or hashed.

Use of system utilities

System utilities are identified, disabled where not necessary, and access to and use of any functional system utilities is strictly controlled.

Session time-out

Timed and password protected screen savers should be used to prevent unauthorised access to data for timed-out sessions. The screen saver should be set to come on at 15 minutes or less.

Information access restrictions

File storage systems should be constructed in order to ensure all and only appropriate personnel have access to a folder which can then be viewed, altered, copied or deleted.

Data file owners are required to password protect all files which contain identifiable patient or staff data.

Sensitive system isolation

All <company name> systems are considered to hold sensitive data and therefore there controls apply to all systems and isolation strategies are not considered appropriate/beneficial.

6. Acceptable use of IT equipment

Prohibited Activities

Staff should not create, store, transfer (from any media or via email) or deliberately receive material that could be judged to be offensive. Offensive/inappropriate material or activities can include:

- Material that is abusive, threatening, serves to harass or bully, discriminates, encourages discrimination on racial/ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Material that may be obscene, indecent or tasteless.
- Material that may cause distress, inconvenience or anxiety.
- Material about illegal activities, including pornography, drugs, computer hacking, militant/extremist behaviour, violence or weapons – unless it is clearly related to your professional role.

If staff receive inappropriate email or become unintentionally connected to a website, which contains offensive or inappropriate material, the member of staff should disconnect from the site immediately and inform their Line Manager.

Deliberate activities with any of the following consequences are prohibited:

- Corruption or inappropriate destruction of data
- Using equipment in a way that makes systems unavailable to others
- Wasting staff effort or computing resources
- Introducing any weakness to, or compromising IT security.

Staff should not download and/or install any software unless authorised by the Chief Executive.

User names and passwords

When staff are logged into a computer under their own username, they must either log out, ‘lock’ the computer or activate a password protected screensaver if they leave it.

Should staff wish to use an unattended computer where a previous user has left their access open, they must log out from that session before they commence their own session.

Staff must not disclose a personal password to anyone. A username and personal password is for one person’s use only. If a member of staff thinks someone else knows their password they must change it immediately and inform the CEO.

Monitoring of activity

Where monitoring of systems takes place to identify system failure/capacity problems and misuse there will not be any monitoring of individual users unless there is justification to do so from general monitoring or concerns raised.

Virus Protection

To protect the practice from computer viruses, no floppy disk, CD or other media should be used unless it has been scanned for known viruses. Should staff receive a virus warning message from a friend or colleague via email, do not forward it on to others, instead notify the CEO verbally.

Personal use of IT equipment

Staff can use IT equipment and facilities for personal use, provided that it is of an appropriate nature, isn't during work time, and cannot be considered as 'excessive' based on the following:

Timing of personal use:

- Staff may make personal use of email & Internet, provided that they only do so during 'unpaid' break periods, such as lunchtime, coffee break or outside of 'general work' hours.

Excessive use:

- Sending large 'attachments' (such as letters, photographs) in personal emails takes up system storage space and communication capacity that is required for practice purposes.
- Sending large numbers of personal emails especially if this is likely to stray into general work hours.
- Downloading large files from the internet.

Large files:

- Any file (or combination) that is larger than 5 Megabytes.

Any breach of this Acceptable Use Policy may be considered as misuse and an investigation may take place.