Morecambe Bay

Primary Care Collaborative

Information Security Policy

Document Reference	POL009
Purpose	To provide a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is adequately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which may otherwise occur.
Author	Mikey Maxwell, IT Consultant and Support
Application/Scope	Organisation-wide
Approval Date	31 July 2023
Review Date (N.B: Review dates may alter if any significant changes are made)	31 July 2026
Version	V3.0
Status	Approved

Key Personnel	
Information Governance Lead	Andrew Giles
Senior Information Risk Owner	Andrew Giles
Caldicott Guardian	Steve McQuillan
Operations Manager	Graeme Redshaw

Morecambe Bay Primary Care Collaborative

CONTENTS

1. INTRODUCTION

1.1 Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

This policy is concerned with the management and security of the Organisation's information assets. An information asset is an item or body of information, an information storage system or an information processing system which is of value to the Organisation.

1.2 Purpose

The purpose of this policy is to provide a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is adequately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which may otherwise occur.

1.3 Scope

The Information Security Policy forms part of a suite of policies that together comprise the Organisation's Information Governance Framework.

The Information Security Policy applies to all information assets which are owned by the Organisation, used by the Organisation for business purposes or which are connected to any networks managed by the Organisation.

The Information Security Policy apply to all services, personnel, facilities and support systems for which the Organisation is directly responsible, as well as any others who may process information on behalf of the Organisation.

For ease of reference, all employees, directors, workers, contractors, volunteers, students or any other person having a working relationship with the Organisation will be referred to as personnel.

From time to time MBPCC may utilise the resources of sub-contractors to deliver contractual obligations. For avoidance of doubt, where a sub-contractor is providing care to patients, as laid out in the contracts between MBPCC and subcontractors, they are solely responsible for delivery of the regulated activity they are providing, and must ensure all their employees operate under their own policies which must meet the relevant CQC standards. MBPCC will seek assurance from all sub-contractors that suitable policies are in place, and may at their discretion request copies of any relevant policies for review and for verification. In such cases this policy document does not apply.

2. PROCEDURE

2.1 Information Security Principles

The following principles underpin this policy:

- Information will be protected in line with all relevant Organisation policies and legislation, notably those relating to data protection, human rights and freedom of information;
- Information assets will be owned by the Senior Information Risk Owner who will be responsible for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset;
- Information will be made available solely to those who have a legitimate need for access;
- All information will be classified according to an appropriate level of security;
- The integrity of information will be maintained;
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification;
- Information will be protected against unauthorised access;
- Compliance with the Information Security Policy will be enforced.

2.2 Governance and Monitoring

Responsibility for the production, maintenance and communication of this policy document lies with the IG Lead.

This policy complements the Information Governance Policy.

The effectiveness of this policy will be monitored via audit and periodic review meetings.

The policy should be reviewed every two years or as a result of organisational or legislative changes that require it to be updated. At this time all previous versions (including electronic copies) should be destroyed.

2.3 Providing a Confidential and Secure Service

Working in open or public areas

Public areas include meeting rooms, reception areas, open offices, corridors, staff kitchens and car parks. Discretion when speaking to others is paramount. During any conversation, do not identify a patient or colleague by name unless absolutely necessary.

- If discussing patients between professionals, the 'need to know' principle applies at all times.
- Discussing personal details whilst others can overhear whilst queuing or in a waiting room is a breach. Offering a private space to talk may be more appropriate.
- Remember a spouse or partner etc. is unable to have access to another patient's details. Parents may not have access if their child is over 16 or, if in the case of a female minor, the girl is deemed Gillick competent.
- Discussing a colleague's health issues is inappropriate and should be given the same confidential treatment as a patient.

Documents

Sensitive documents should be secured immediately after use and not left unattended. 80% of disclosures of sensitive information are due to unauthorised persons seeing information on staff boards, lying around during breaks and not being cleared away at the end of a working day.

Do not display any signs relating to the location of storage of sensitive documents and do not leave keys for document cupboards in unsecured places.

Photocopiers

The use of a photocopier should only be granted to authorised personnel to minimise secure information from being copied.

Consideration should be given to where the machine is situated (can it be relocated to a secure room?) and whether it can be used without an access code.

Faxes and post

For information being transmitted by either faxes or direct mail, try to keep the amount of identifiable or confidential details to a minimum. As a default, try not to send identifiable or confidential information unless absolutely necessary. Ensure that confidential information is not put in general waste bins. Dispose of it carefully e.g. put in confidential waste bags, shredded or locked away until it can be disposed of securely.

Only use a "Safe Haven" fax machine to send to or receive. These are fax machines kept in a secure room and which have limited access, or are locked in a secure cupboard.

Use a fax header/cover sheet which includes:

- the organisation's name;
- the department;
- the department it is being sent to;
- the recipient's name;
- date and time;
- number of pages;
- a telephone contact number;
- the receiving fax number;
- "Private and Confidential", where appropriate.

Double check fax numbers. Do this every time, even if the number is in the machine's memory.

Try to send information to a named person rather than a general department. If it is not known who the information needs to go to or if the information contained in the fax is of a sensitive nature, ring ahead to find out or let the intended person know they will be receiving a fax which contains confidential details. It may also be reasonable to ask them to ring back to confirm receipt and/or also request a report sheet to confirm transmission.

If there is a problem when sending a fax, telephone the person or department and check the number. Do not to leave the document unattended on the fax machine.

Check fax machines for incoming faxes regularly throughout the day. Consider allocating responsibility for this to a designated person/deputy. There may be confidential details on the fax waiting for collection. Keep the area around the machine tidy and throw away waste paper.

Remember to mark all post as 'Confidential' if it contains patient or employee details and seal the envelope, even internal post which is in transit envelopes.

Avoid opening post in public areas e.g. reception, where anyone can read information left unattended, even momentarily.

Telephones

Not only should the Organisation be aware of the location of telephones and who might be within earshot, care should also be taken as to the siting of, and access to, the internal telephone directory. An internal directory can pinpoint where secure or sensitive information is kept.

When handling telephone queries, the following should be observed:

- Always check who is on the other end of the phone;
- If necessary ask the enquirer for a number they can be contacted on;
- In some cases, the procedures may make it compulsory to only disclose information on a "ring back" basis. Always think about whether the information has been authorised to allow disclosure to the enquirer;
- Only disclose information if there is the authority to do so;
- Only disclose necessary information. Even if it is information that the enquirer would normally be entitled to, is it appropriate to disclose it in the context of the current query?
- If in doubt about anything, ask the manager, not a colleague;
- Do not be pressurised into giving out information that should not be given out;
- If challenged by the enquirer for not giving out information, remain calm and polite but clearly state that authority is not available to disclose the information they are asking for;
- If it is possible for the enquirer to request the information in writing, consider offering this as an option;
- Alternatively, offer for the manager to speak to them, preferably by ringing them back. Do not just transfer the caller. The manager needs to be fully informed of the situation before dealing with the query.

Scanning equipment

Similar directives to those described for photocopiers apply to the scanning equipment.

In line with the requirements of the Clinical Record Keeping policy, where a specific back-up procedure is performed, this should include regular spot checks on a series of images to ensure the accuracy of content and replication.

2.4 Personnel

Staff

Staff should be issued with identification badges, which should be worn at all times.

Visitors

Visitors may not always be wearing badges but it is imperative that their credentials are verified, as incidences of bogus staff are becoming more frequent. Temporary staff and visitors of all kinds should be allocated a special badge so that they can be recognised as such. Visitors, including maintenance staff, should book in at reception or point of entry and, where applicable, be escorted.

Staff who notice anyone who does not display an authorisation badge in a controlled location should report this to a responsible person. Always be mindful of personal safety.

Staff departures

When staff leave the Organisation, depending on the circumstances, it may be necessary to ensure that keys are returned and intruder alarm codes are changed.

Access to systems

Where staff are recruited to a role which requires access to clinical systems containing patient records it is important that the following points are considered:

- checks on an applicant's ID are made during recruitment;
- offers of employment are dependent on the applicant's ability to meet and continue to meet all requirements relating to confidentiality and IG;
- induction processes include training on IG and confidentiality;
- staff must sign to acknowledge that they have read and understood the policies and procedures relating to IG and confidentiality.

System access credentials must not be shared and must only be known by the person they were issued to.

System access credentials should be treated with care and precautions should be taken against loss or damage. Lost, stolen or compromised credentials should be reported to the Operations Manager as soon as possible. The Operations Manager will ensure the account is secured and carry out an access audit to determine if unauthorised access has occurred.

If the Operations Manager is aware or made aware of any breaches in the use system access credentials and associated user privileges, they should disable the access pending a full investigation.

2.5 Preventing Equipment Loss

All terminals and other computer equipment shall, wherever possible and practical, be located in rooms where windows and doors can be and shall be locked when staff are not present. In administrative areas which patients and other members of the public normally have cause to enter, access shall be strictly controlled.

If equipment cannot be located within a room as described above, it shall be located, wherever possible and practical, in an area which is always supervised, and where patients and other members of the public have no cause to enter unless invited by a member of staff.

Equipment which, through force of necessity must be located in an area to which the general public have open access and which may be unsupervised for prolonged intervals, shall be physically protected against opportunistic theft.

All portable equipment shall be clearly and indelibly marked to indicate that it is the property of the Organisation. Where possible and practical such equipment shall be locked away when not in use.

Portable equipment shall not be removed from the Organisation's premises without written authority from the Operations Manager. This will be granted only on the understanding that:

- the employee assumes full responsibility and liability for any loss or damage, however caused;
- no item of equipment is left in an unattended vehicle;
- equipment will only be used for bona fide Organisation business;
- equipment will only be used by Organisation employees:
- equipment is not removed beyond the United Kingdom.

All equipment, including portable, shall be entered on an asset register, which shall also record the individual to whom it is allocated or, in the case of non-portable equipment, the room in which it is situated. Changes to these allocations shall be logged on the register.

Each user shall ensure that all relevant PCs and network terminals are physically secured in accordance with the recommendations of this Security Policy.

If deemed appropriate, closed circuit television (CCTV) cameras shall be sited at suitable locations throughout the Organisation to monitor the access and activity at places of particular sensitivity, wherever possible.

2.6 Use of Computers

Access to Computer Systems

The biggest threat to security is staff leaving computers unattended and logged on. Never leave sensitive information on the screen. All computer screens must be positioned so that they cannot be overlooked by members of the public or unauthorised personnel.

Where patients and other members of the public are able to view the output on a screen, whether as a passer-by or by invitation, staff shall exercise great care to ensure that unauthorised disclosure does not occur, for example, clearing a displayed patient record from the screen before a new patient enters the consulting room. Care must also be exercised to ensure that passwords are not disclosed to others (staff or public) who may observe the use of the keyboard.

The Operations Manager is responsible for enabling staff access to systems. Access to data should be controlled further by adopting a rigorous password policy and, where appropriate, use of password-protected screen-savers. Staff must be given access only to the areas of the system consistent with their role. This includes any locum or temporary employees. An up-to-date list of staff access levels should be kept in a secure location.

Each member of the Organisation and other users of the systems must have a unique username and password. Usernames and passwords allowing access to any system must be kept confidential. Each user must log on with their own username and password and must log out or lock the computer when not present. Passwords are not shareable and staff should be made aware that passwords should be changed if they think it has been guessed or used by someone else.

Systems access should be disabled when staff leave the Organisation.

No member of staff or visitor shall install software from any source without the express permission of the IG Lead. Unauthorised loading of unchecked software will be considered a serious disciplinary offence.

Software appropriate to the running of the Organisation should not be installed without prior authorisation from IG Lead.

No member of staff or visitor shall insert any removable data devices without the express permission of the IG Lead.

If any member of staff is permitted remote access to the Organisation network and systems, it is imperative that unauthorised access to information is prevented when the laptop is not within the Organisation premises.

Computer backup procedures

The IG Lead shall be responsible for taking and securing back-ups for all data and software relevant to the systems and, in the interests of the Organisation; they are to ensure that this is properly done on a regular and routine basis. A comprehensive backup procedure must be documented and distributed to all personnel.

The Organisation uses the EMIS Web clinical system which is backed up centrally.

Essential Organisation data will be backed up on a daily basis. Backups should be verified weekly. Any backup on removable media should be encrypted.

Data recovery procedures for the clinical system

The Organisation uses the EMIS Web clinical system which would be recovered centrally.

Laptop computers/PDAs/mobile telephones/portable data storage

No confidential information should be stored in any of this media type unless it is encrypted. Such items should never be left unattended in a public place, in a car or in an office without adequate security. Children or partners should not be allowed to use these items. All such devices must have an access control measure such as a PIN or password in order to access them.

Protection from malicious software

If you suspect the computer may be infected, note any suspicious messages or activities and inform the IG Lead or Operations Manager immediately.

Do read carefully any virus warnings from the IG Lead. Do not open virus warnings from sources other than the IG Lead. Do not forward any virus warnings from any source and always ask the IG Lead for advice if a warning is received – it may be a hoax.

Check any disks for viruses before using them on any PC. Ensure that anyone introducing floppy disks/CDs/USBs onto the system has validated that the disk is clean and free from viruses. Do not use freeware or shareware from any source without appropriate authorisation.

Educate the users of the system to be vigilant in the use of email, taking special care when opening unexpected attachments from known or unknown sources. If the subject line appears strange always check with the sender by phone if you are unsure. Do not run executable attachments.

Anti-virus software

Anti-virus software contains two elements; the 'engine' and the virus definition file. The virus definition file is a database of all known viruses and is used by the engine to compare against files being scanned on the system. If a match is found, the system has a virus.

It is imperative that the Organisation employs a robust and reliable anti-virus procedure to combat the genuine threat of data loss from virus attack. Viruses can quickly spread from machine to machine on a network, so a single incident can soon cause a devastating effect on the whole system.

Each machine should be configured to perform an anti-virus scan daily. The anti-virus software must be running 'in the background' at all times during normal operation of the machine.

It is imperative that the anti-virus application is kept regularly updated, as there are several hundred new viruses discovered each month. The virus definition files are updated by manufacturers at least once per week – more regularly if a batch of new viruses are discovered.

If a virus has been contracted, the virus definitions that the system is using are probably out-of-date. Disconnect the computer from the network and report the problem to the IG Lead immediately.

If the virus scan finds an infection, it will give the name of the virus or viruses that have been contracted. Removal instruction may also be offered. Viruses vary in severity. Some are easy to eliminate and repair. Others can be very nasty and repairing their damage could involve some complex reprogramming.

How to recognise virus attack

Viruses often cause erratic behaviour. Smiley faces may pop up, the screen may turn blank, the computer may crash, or it may constantly reboot. The trigger that activates the virus can be almost anything. It can be activated the minute it is installed or at the next start up. In some cases, a virus can reside inside the computer in an inactive state, waiting for a certain event/date to happen. From the moment the virus infiltrated, to the time that it made itself known, the virus may have spread to others.

Malicious software can take many forms:

- A 'logic bomb' waits on the computer and then causes damage to it when triggered by an event like a specific time or date - like the Millennium Bug happening on New Year's Eve 1999.
- A 'file virus' uses program files to get into the computer and then it copies itself.
- A 'worm' does not damage files, but copies itself endlessly across computer networks and the internet which slows them down and frustrates computer users.
- A 'boot sector virus' damages the specific files that the computer needs to start up.
- A 'macro virus' infects by using special codes found in word processing and spreadsheet files.
- A 'Trojan horse' is a malicious computer code that pretends to be a game or other interesting program that damages the PC as soon as it is opened.
- Spyware (sometimes called Adware) is uninvited software that is transferred to the computer without explicit knowledge. It often piggybacks on software that is downloaded from the Internet. Spyware causes erratic behaviour in a computer that is very similar to the behaviour caused by viruses. Often spyware is characterised by unusual windows popping up, but the computer can be infected by spyware even if there are no annoying pop ups. If

virus scan shows no viruses, but the computer is still acting strangely, spyware should be suspected.

Spotting the symptoms

- If the hard disk or removable disk seem to be working at full speed to do simple tasks, or when they should be idle.
- If new or regularly used, removable disks become unusable.
- If the computer is operating slower than normal.
- If a computer program cannot be opened, or if a program shuts down on its own.
- If unusual error messages pop-up on the screen. To check if this is genuine or a virus, it is always worth copying the error into a search engine to find advice from experts on the Internet.
- Unusually slow download speeds can also indicate that the software running the connection has been infected.
- A virus could also be responsible for any strange screen activity that might be happening.

Responding to a virus attack

The anti-virus application should report on the severity of the attack and whether it has successfully prevented the virus from infecting the system. The IG Lead must check the report and apply the necessary steps in accordance with the severity and success of the attack.

In the event of the anti-virus application capturing and quarantining the virus with no further infection noted, it should be possible to resume normal use of the system – however the IG Lead must still log the attack.

If the anti-virus procedures do not work, disconnect the affected computer from the network by unplugging the network cable at the wall point. Respond to any request by the anti-virus software to Clean or Quarantine the infected files. If this fails, seek help from the IG Lead. Do not shut down the machine or attempt to clean the computer.

If the virus came via email, inform the sender immediately. Email-borne viruses can spread by attaching themselves to messages that are then sent to all members of an address book, so the virus could be sent to hundreds of users at a stroke. The sender must be told in order to stop further spread of the virus.

If the virus came in through a floppy disk/CD/USB, ensure the disk is quarantined pending further investigation.

Some viruses can lay dormant for many weeks before activating, so the Organisation backups must be checked for contamination.

Use of email and internet

Personal use of the Organisation's computer system for email and internet access is permitted during breaks.

Use of the Organisation IT systems to access inappropriate or offensive websites, or to send inappropriate or offensive material, is expressly forbidden.

The use of public Wi-Fi on company equipment is forbidden unless using a VPN.

Emails often go astray. They can be opened by someone other than the intended recipient if sent to the wrong person and messages cannot be controlled once sent. Remember that emails are recorded and can be presented as evidence. All laws relating to written communications such as copyright and defamation also apply to emails.

Staff use of the internet and the contents of email folders may be monitored.

Sending email

- Use a meaningful subject line so the recipient knows the mail is genuine and not a hoax or virus;
- Use terms consistent with other business communications;
- Carefully review the message before sending it and double-check to whom it is being sent;
- Be very careful when selecting recipients from an address list – there may be many people with the same name;
- Use distribution lists sensibly;
- Confidential information may only be sent from an NHSMail address to another NHSMail address (those ending @nhs.net);
- Do not send 'chain' emails;
- Keep personal use to a minimum.

Receiving Email

- Be very careful opening mail with attachments;
- Copy emails which need to be saved;
- Remember to delete unwanted mail regularly from inboxes, sent boxes and deleted boxes;
- Do not print emails unless absolutely necessary.

Internet usage

- Internet usage may be monitored and can be traced, to time, location and user name;
- Connecting to sites holding offensive material is a serious breach of security and could result in dismissal. If unintentional access to such a site occurs, disconnect immediately and inform the IG Lead;
- If you are unsure about permitted access, ask the IG Lead;
- If internet use is required and the previous user has left it logged on, first log out and then log back on. Technically, this is a security breach and should be reported;
- Always log out after use;
- Do not download anything that may breach copyright or other laws. If in doubt, ask;
- Do not download and install any program without formal authorisation.

3. DEFINITIONS/GLOSSARY OF TERMS

Abbreviation or Term	Definition
MBPCC	Morecambe Bay Primary Care Collaborative
CQC	Care Quality Commission
IG	Information Governance
EMIS	Egton Medical Information Systems

CCTV	Closed circuit television
PDA's	Personal digital assistant

4. CONSULTATION WITH STAFF, PRACTICES AND PATIENTS

Name	Job Title	Date Consulted

5. DISSEMINATION/TRAINING PLAN

Action by	Action Required	Implementation Date
Jo Knight/Boyana Konar	Upload policy to MBPCC website	30/09/2020
Jo Knight	Delete out of date copies and host current copy on Federation G Drive (supporting induction process), updating Policy tracker	30/09/2020
Liz Stedman	Upload to TeamNet	Jan 2021
Liz Stedman	Upload to TeamNet/website	June 2021

6. AMENDMENT HISTORY

Version No.	Date of Issue	Section/Page changed	Description of change	Review Date
V1.0	27/08/2020	All	New policy	27/08/2023
V1.1	20/09/2020	All	New format	27/08/2023
V1.2	19/01/2021	Page 13	Additional Definitions/Glossary of Terms added	
V2.0	15/06/2021	Review	Approved by the Board	15/06/2023
V2.1		Key Personnel Pg1.	Named Operations Manager added	
V3.0	31/07/2023		Approved by the Board	31/07/2026