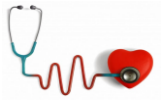
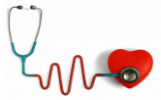
Bedford Street & Furzton Medical Centre

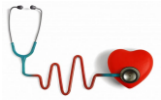


K82039

Contents



Bedford Street & Furzton Medical Centre



K82039

1. Introduction

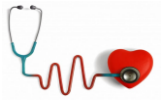
1.1. Information and cyber security has critical importance to NHS service users and to patient care, information assets and other related business processes. High quality information underpins the delivery of high quality evidence – based healthcare. Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to the PRACTICE, therefore the organisation must ensure that the information is properly protected and is reliably available.

1.2. Information security is primarily about people, but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Bullet list (remove if not using) Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the PRACTICE is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff (as defined in the scope) when working on the PRACTICE business.
- A strengthened position in the event of any legal action that may be taken against the PRACTICE (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that electronic communications, systems and removable media are used as intended.

2. Purpose / Policy Statement

2.1. The purpose of this policy is to protect, to a consistently high standard, all information assets, including patient and staff records and other NHS corporate information, from all potentially damaging threats (including cyber threats), whether internal or external, deliberate or accidental, to ensure the integrity of the PRACTICE's systems including reliability, availability, correctness and completeness of data, to protect the

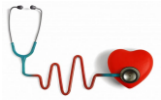


PRACTICE and their staff from allegations of inappropriate or profligate use and to ensure the privacy of electronic communications to and from PRACTICE staff.

2.2. The PRACTICE has a legal obligation to ensure that there is adequate provision for the security management of the information resources the organisation own, control, or use. Any action taken to comply with Information & Cyber Security guidance will not amount to discrimination because of protected characteristics as set out in the Equality Act 2010.

3. Definitions

- Asset – Anything that has value to the organisation, their business operations and continuity.
- Authentication – The organisation must ensure that the identity of a subject or resource is the one claimed.
- Availability – The property of being accessible and usable upon demand by an authorised entity.
- Business Impact – The result of an information security incident on business functions and the effect that a business interruption might have upon them.
- Confidentiality – Keeping, or being kept, private Information is not made available or disclosed to unauthorised individuals, entities or processes.
- Cyber Security – Information and Cyber Security concerns the comprehensive risk management, protection and resilience of data processing and the digital networks that connect them.
- Electronic Communications – For the purpose of this policy electronic communication facilities include but are not limited to Electronic Mail (e-mail); Internet usage; Remote / home working; Use of Personal Computers (PCs), laptops, tablets, portable devices; Telephone usage (including mobile phones, dictaphones, voicemail)
- Impact – The result of an information security incident, caused by threat, which affects assets.
- Information Assurance – The confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.
- Instant Messaging – Instant messaging (IM) technology is a type of online chat that offers real-time text transmission over the Internet. Short messages are typically transmitted between two parties, or within a group of users.



- Personal Confidential Data / Person Identifiable Data (PCD / PID) – where an individual can be identified (a) From the data, or (b) From the data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (as per Data Protection legislation).
- Portable Devices – The use of portable devices includes Laptops; Notebooks; iPads / iPods or other tablets capable of connecting to a computing device and storing information; Smartphones
- Portable Storage Devices – External hard disk drive; USB memory or flash drive (memory sticks or cards); Solid State memory cards; Future technologies such as Google Glass.
- Remote Working – Remote working is accessing the organisation resources whilst working away from a normal fixed place of work.

4. Roles and Responsibilities

4.1. All PRACTICE Employees

4.1.1. All staff are required to comply with information security procedures including the maintenance of data confidentiality and data integrity. Each member of staff is responsible for the operational security of the information systems they use. Failure to do so may result in disciplinary action.

4.1.2. It is important that software on the PCs / systems used for work purposes must not be copied and used for personal use that may infringe on the organisation's system.

4.1.3. Staff must not load software onto their computer before first seeking advice / agreement from the IG Lead or ICT service provider [Name of Provider]

4.1.4.

4.1.5. To ensure business continuity in the event of individual unavailability, all staff must ensure that information belonging to the organisation should not be stored on personal drives, in "My Documents", on the desktop or in e-mail accounts (other than generic email accounts).

4.2. Senior Information Risk Owner (SIRO)

4.2.1. The role of the Senior Information Risk Owner (SIRO) is further described within the PRACTICEs Information Governance Framework and Policy.

4.2.2. The SIRO is responsible for leading on Information Risk and for overseeing the development of an Information Risk Policy.

4.2.3. The SIRO is also responsible for ensuring the corporate risk management process includes all aspects of information risk and for guaranteeing the PRACTICE Board / Governing Body is adequately briefed on information risk issues.

4.3. Caldicott Guardian

4.3.1. The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients/service-user's information and enabling appropriate information sharing.

4.3.2. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

4.4. Information Asset Owners (IAOs)

4.4.1. Information Asset Owners (IAOs) will act as nominated owner of one or more information assets. Their responsibilities will include:

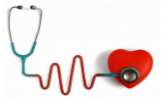
- Documenting, understanding and monitoring what information assets are held and for what purpose, how information is created, amended or added to, who has access to the information and why.
- Identifying information necessary in order to respond to incidents or recover from a disaster affecting the information asset.
- Taking ownership via input, of their department / service area Information Asset Register, carrying out risk assessments on their local asset and management processes for the information assets they own, including the identification, review and prioritisation of perceived risk and oversight of actions agreed to mitigate those risks.
- Providing support to the SIRO to maintain awareness of risks to all information assets.
- Ensuring their staff are aware of, and comply with, Information Governance working practices.

4.5. Line Managers

4.5.1. Line Managers will take responsibility for ensuring that their staff are aware of:-

- Information security policies applicable in their work areas
- Personal responsibilities for information security, includes appropriate use of electronic communications
- How to access advice on information security matters

4.5.2. Line managers are responsible for the security of their physical environments where information is processed or stored.



5. Policy Detail

5.1. Process Requirements

5.1.1. This policy will achieve a consistent approach to the security management of information throughout the PRACTICE and will aim to deliver continuous business capability and minimise both the likelihood of occurrence and the impacts of information security incidents.

5.1.2. Security of our information is paramount, and the protective measures put in place must ensure that Information Governance (IG) requirements are satisfied. The aim of this process is maintaining the confidentiality, integrity and availability of PRACTICE information. To conform to the assertions of the NHS Digital Data Security and Protection Toolkit (DSPT) the PRACTICE shall:

- Maintain the Confidentiality of Personal Information including patients and staff (as defined in the scope) identifiable information by protecting it in accordance with NHS Information Security Code of Practice, Data Protection legislation, Caldicott Principles and other legal and regulatory framework criteria.
- Ensure the integrity of the PRACTICE information by developing, monitoring and maintaining it to a satisfactory level of quality for use within the relevant areas.

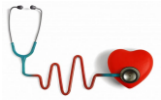
5.1.3. Implement the necessary measures to maintain availability of the PRACTICE information systems and services. This includes putting in place contingency measures to ensure the minimum of disruption caused to the PRACTICE information systems and services.

5.1.4. Alongside this Information and Cyber Security policy, the PRACTICE will provide specific guidance and instruction to staff in policies and procedural documents, such as Information Governance Framework & Policy, Records Management and Information Lifecycle Policy, Information Sharing Policy, Access to Information Policy and the IG Resource Guide.

5.1.5. All IG policies and the IG Resource Guide are available on the staff intranet or PRACTICE shared drive, public website and from the IG team.

5.2. Physical Security

5.2.1. The physical security of the organisation's information is the responsibility of all staff. The protection of both personal and non-personal information is paramount in maintaining confidentiality and users of the organisation's information must comply with the suite of Information Governance documentation. This is a local information security policy to protect the information stored, processed and exchanged between the PRACTICE and its partner organisations.



5.2.2. The physical environment must be recognised as providing a layer of protection to data and information. This is achieved by the following means:

- Controlling access to sites, buildings and offices
- Ensuring desks and work areas are clear at the end of each day
- Use of locked cabinets within offices to restrict access to information
- Checking that visitors to sites are authorised to be there
- Always wearing your ID badge when on site.
- Ensuring that when information and / or devices are carried off site, they are stored securely and out of sight during transit

5.2.3. Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions.

5.3. Mobile Devices

5.3.1. PRACTICE owned portable devices, for example, laptops must be encrypted and kept in locked storage. Removable media must be encrypted and must not be the only source of the information (that is the information must also be stored in a secure folder on the shared drive). Such media must be kept in locked storage.

5.3.2. Removable media must only be installed by the IT service provider, on PRACTICE owned devices. Personally owned removable media devices must not be used to store or transfer any confidential information without seeking permission. Each user of such media is responsible for the appropriate use and security of data stored on the media.

5.4. Viruses and Malware

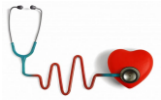
5.4.1. All IT equipment used by staff is protected by countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with this policy.

5.4.2. Users shall not install software on the organisation’s property without permission from the IT service provider.

5.5. Preventing Information Security Breaches

5.5.1. Each department/service area is responsible for regularly monitoring the information they hold and use.

5.5.2. An annual mapping exercise of information flows in and out of the teams will be undertaken, along with maintenance of an Information Asset Register. These



exercises will allow any information risks to be identified by each team and appropriate action to mitigate those risks should be taken.

5.5.3. It is the responsibility of the Information Asset Owner (IAO) to ensure that this takes place.

5.6. Protection Against Unauthorised Access or Disclosure

5.6.1. Staff have a responsibility to ensure that information is kept secure when being processed or transferred, by adhering to the following:

- Screens should be locked when unattended even for short periods of time
- Guidance on protecting and securing Information, Information systems and portable devices is covered in this Policy.
- Guidance surrounding passwords, complexity and good practice as available in Appendix B. Guidance provided on the use of fax, 'phones and post can be found within the Records Management and Information Lifecycle Policy.
- The IG Resource Guide, which provides additional guidance.

5.6.2. The IT service provider, Arden & GEM CSU, will ensure that all computer software supplied / used, and installed on PRACTICE owned devices, is regulated by license agreements and that new operational software is quality assured.

5.6.3. The PRACTICE will ensure that paper information is secure by following adequate records management procedures and processes. Staff should have access to secure storage areas and if possible, a clear desk routine should be followed.

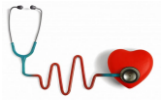
5.6.4. Should a legitimate need arise for local storage or a non-routine transfer of confidential information then a risk assessment must be undertaken first, the justification approved by the Caldicott Guardian and recorded by the line manager. All staff must also ensure when moving away from desks that they do not leave person identifiable / sensitive information available for others to view by putting it in a drawer or covering it up.

5.6.5. Any non-routine bulk extracts (50+ records) or transfers of particularly confidential or sensitive data must be authorised by the responsible Information Asset Owner (IAO) for the work area and may require approval by the Senior Information Risk Owner (SIRO).

5.7. Passwords

5.7.1. All staff have a duty to ensure information and systems are protected against unauthorised access.

5.7.2. Guidance surrounding passwords, complexity and good practice as available in Appendix B.



5.8. Potential or Actual Information Security Breaches

5.8.1. All staff are responsible for ensuring that no potential or actual security breaches occur as a result of their actions.

5.8.2. The IAO must be informed of all security issues in order to ensure that the appropriate investigations are carried out.

5.8.3. Depending on the impact of the incident, external organisations such as NHS Digital (formerly HSCIC), NHS England and the Information Commissioner's Office (ICO) may be informed.

5.8.4. The resulting root cause analysis (RCA) report will specify details of the suspected incident, the assets affected or compromised and the investigation conducted. Recovery / contingency plans, damage and risk classification and recommendations will be provided.

5.8.5. All incidents will be investigated immediately and reported in a timescale appropriate to the initial risk assessment. Full guidance is available in the Breach Reporting Policy.

5.8.6. Reports and recommendations following security breaches will be approved and monitored by the DPO.

5.9. Risk

5.9.1. The PRACTICE will ensure that adequate audit provision is in place to ensure continuing effectiveness of information security management arrangements.

5.9.2. Any security measures must be viewed as necessary protection against a risk of an event occurring or to reduce the impact of such an incident. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

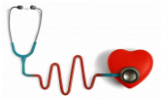
- The threat of something damaging the confidentiality, integrity or availability of information held on systems or manual records.
- The impact that such a threat would have if it occurred.
- The likelihood of such a threat occurring.

5.9.3. All staff should consider the risks associated with the computers they use and the information that is held on them, as well as information held in manual records

5.9.4. All staff are responsible for reporting any apparent shortcomings of security measures currently employed to address these risks to the risk lead within the organisation.

5.10. Information Disposal

5.10.1. Computer assets must be disposed of in accordance with the IT service providers disposal of confidential waste procedure. This includes removable computer media such as tapes and disks.



5.10.2. All data storage devices must be purged of sensitive data before disposal. Where this is not possible, the equipment or media must be destroyed by a technical waste service provider.

5.10.3. For further information, please contact the IT service provider.

5.10.4. Printed matter should be confidentially destroyed using an appropriate method such as shredding.

5.10.5. The Records Management and Information Lifecycle policy provides further guidance.

5.11. Access Controls

5.11.1. Only authorised personnel who have a justified and approved business need must be given access to restricted areas or systems containing information or data.

5.11.2. User access controls ensure information is restricted to authorised users who have a bona-fide business need to access the information.

5.11.3. Authorisation to use an application will be dependent upon the availability of a license from the supplier.

5.12. Use and Installation of Software

5.12.1. The IT service provider –[Name of Provider] will ensure that:

- Security issues are considered and documented during the requirements phase and the procurement phase of all system procurements and developments. Minimum security standards must be incorporated in all new systems.
- System tests and live data are separated and adequately protected. All changes to the system must pass through a formal change control procedure.
- Computer assets such as removable media, backup tapes and disks are adequately disposed of.

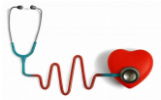
5.13. Data and Information Backup

5.13.1. [Name of Provider] will ensure that data located upon network servers is backed up in accordance with the written network back-up procedure.

5.13.2. Such information is to be stored off-site as required to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.

5.14. Use of Electronic Communications

5.14.1. The PRACTICE's primary aim in providing electronic communication facilities is to support and enable the delivery of the highest quality service to patients and service users.



5.14.2. In the event of any untoward activity the PRACTICE will proceed to act in accordance with the organisation's disciplinary procedures.

5.14.3. The PRACTICE will always comply with any reasonable request from law enforcement and regulatory agencies for logs, diaries and archives on an individual's electronic communication activities.

5.14.4. Members of staff are expected to conduct themselves honestly and respect copyright, software licensing rules, property rights, the human rights and privacy of users. When using electronic communications members of staff are expected to use common sense to ensure that the use of these facilities does not leave the PRACTICE or themselves open to a legal challenge.

5.14.5. The PRACTICE does not accept liability for any fraud or theft that results from personal use of the PRACTICE's electronic communications facilities.

5.15. Acceptable use of internet and e-mail

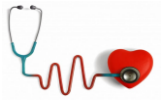
5.15.1. Members of staff are encouraged to use the internet and e-mails to further the goals and objectives of the PRACTICE. The types of activities which are encouraged include:

- Communicating with colleagues, business partners of the PRACTICE and suppliers within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Personal educational research and recreational use of internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, or the work of others.

5.16. Unacceptable use of internet and e-mail

5.16.1. Personal internet and e-mail use should not interfere with others productive use of resources. Internet and e-mail use must comply with all UK laws, PRACTICE policies and contracts. This includes, but is not limited to, the following:

- The internet must not be used for illegal purposes, including (but not limited to) copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation and bullying, forgery, impersonation, gambling or computer tampering (for example spreading computer viruses), offensive, abusive, bullying, harassing, homophobic, sexist, racist, hateful or otherwise discriminatory material;
- Use of the internet in a manner that is not consistent with the strategic objectives or values of the PRACTICE, misrepresents the organisation or violates any of its policies.



- Access to the PRACTICE's resources or network facilities for those who are not staff are prohibited, as well as the use for mass unsolicited mailings, uploading and downloading of files for personal use, access to pornographic sites, gaming, dissemination of chain letters and competitive commercial activity unless pre-approved by the PRACTICE.
- Staff should not view, copy, alter or destroy data, software, documentation or data communications belonging to the PRACTICE or other staff without authorised permission.

5.16.2. Any e-mail use that includes creating, sending and forwarding messages containing any of the following may be considered gross misconduct:

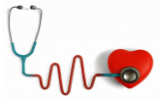
- Material that brings the organisation or a colleague into disrepute.
- Pornographic, obscene, indecent or sexually explicit material .
- Illegal material .
- Material which makes improper or defamatory reference to the protected characteristics groups as defined by the Equality Act 2010.
- The use of copyright material or the work of third parties without prior consent.
- Unsolicited commercial or personal advertising material.
- Viruses, spy-ware or mal-ware.
- Personal opinions represented as that of the PRACTICE.
- "Mass mailing" information, except for important PRACTICE business.

5.17. Email – Good Housekeeping

5.17.1. E-mail capacity is not unlimited. All nhs.net e-mail accounts will issue a warning when the mailbox is 90% full. Once full you will not be able to send but will continue to be able to receive a further 200MB of mail before inbound messages will be rejected. Therefore, regular housekeeping is required and e-mails should be deleted, archived or stored as appropriate.

5.17.2. In the interests of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files, other than those necessary for business purposes and which cannot be accessed through a shared drive. The size and restriction on sending a single email is 20MB. Sending e-mails with large attachments can adversely impact the performance of the network.

5.17.3. Senders should be aware of the general availability of e-mail addresses, so that urgent information does not lie unread and a reply indicator should be used. Staff



should therefore make appropriate use of the Out of Office Assistant facility indicating date of return and alternative contact details.

5.17.4. Facilities for diverting e-mails during staff absences or for administrators or personal assistants having access to a manager's e-mail inbox should be used within the constraints of confidentiality.

5.18. Access to Another Individuals Account

5.18.1. In circumstances (such as sick leave or personal emergencies), where delegated access has not been given and there is an immediate business need to have access to information held in a user's account, then the following process should be followed:

- The senior manager of the nominated staff should contact the IT service provider for access.
- Based on the business need, in the case of access to a mailbox, the request should clearly state what access is required (i.e. inbox, entire email account); in the case of access to a personal drive, the request should state if access to the entire personal drive is required, or if access to a specific file is required.
- Requests will be reviewed and considered by the PRACTICE Caldicott Guardian (or nominated deputy).
- Consideration should be given as to whether staff should be informed of the access, the business justification and the nominated individual who had this and the period of time.

5.19. Instant Messaging

5.19.1. Instant messaging (IM), where available, should be used for business related communications only.

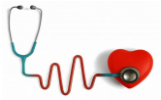
5.19.2. It is not intended to replace email, but to enable short conversations where the content is not required to be retained or audited, e.g. I'm running late, please postpone our meeting by 10mins, you mentioned you visited X practice last week- do they have a practice manager? Etc;

5.19.3. IM Creates a written record which may be monitored / audited as appropriate. Be aware that stored conversations may be used:

- In Court
- In response to Freedom of Information (FOI) requests
- In response to Data Protection requests (subject access)
- In disciplinary / misconduct investigations and proceedings

5.19.4. When using IM:

- you should keep conversations professional and use appropriate language.



- ensure that you do not send or disclose any person identifiable data (PID), confidential information, person sensitive or business sensitive data.
- make sure that any information or discussions with a set retention period, or that must be kept for auditing purposes, are not discussed over IM.
- do not send attachments over IM (even if the system allows it).
- you should ensure that it is not used for personal business, social discussions, advertising / marketing or forwarding of chain messages.
- never use text or materials deemed offensive, obscene, illegal, indecent, pornographic, etc.

5.19.5. IM is subject to all IG and IT Policies. Any misconduct in relation to IM will be dealt with under the PRACTICE's disciplinary procedures.

5.20. Microsoft Teams Video Conferencing

5.20.1. Video conferencing (VC) should be used for business related purposes only.

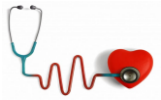
5.20.2. Users should be mindful of where they make / receive a video call to ensure person identifiable and / or sensitive information remains confidential and cannot be seen or overheard by others.

5.20.3. It is possible to share files over Teams, however, before sharing any person identifiable and / or sensitive information, users should ensure all recipients are entitled to the information.

5.21. Portable Computing Devices

5.21.1. All staff authorised to use the PRACTICE's portable computing devices must:

- Take all reasonable care to prevent the theft or loss of these devices.
- Ensure that the devices are not left unattended for example in a public place or in vehicles.
- Take extra vigilance when using any portable computing device during journeys on public transport to avoid the risk of its theft or unauthorised disclosure of the organisation's stored information by a third party "overlooking".
- Ensure that 'non-authorised' users are not given access to the device or the data it contains.
- Ensure that the portable device is encrypted.



- Ensure that any suspected or actual breaches of security are reported to the assigned Information Asset Owner, the Head of Corporate Governance and the Head of Information Governance.
- Ensure that unauthorised software is not installed on the device.
- Ensure that information is virus checked before transferring onto the organisation's computers. This will be done automatically for information that is sent via e-mail.

5.21.2. Where it is not possible to encrypt sensitive / personal information, the advice of the assigned Information Asset Administrator (IAA) and the Information Governance Team is to be sought and, where no solution can be found, the risk is to be articulated to the Head of Corporate Governance and Senior Information Risk Owner (SIRO) in the PRACTICE.

5.21.3. Confidential information should only be stored on a portable device with the permission from the assigned Information Asset Owner (IAO). This should be recorded on the department's Information Asset Register and an updated copy sent to the Information Governance Team.

5.21.4. Where available, only NHS Digital (formerly HSCIC) approved encryption products are to be utilised to secure sensitive / personal information. Where no such products exist the advice of the assigned IAO / IAA or the Information Governance Team is to be sought in all cases.

5.21.5. Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available, and the contents must be encrypted.

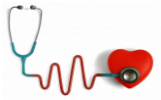
5.21.6. Use of non-corporate portable devices - Only PRACTICE assets (or those on an approved list) may be connected to the network. If in doubt, please refer to the IT Department.

5.21.7. Return of portable devices - Staff including temporary or contract staff leaving the PRACTICE should return the portable device to the Corporate Business Manager, or their line manager, IAO, IAA or the CWS Head of Strategic IT. All media containing the organisation's information must be returned for retention or appropriate destruction..

5.22. Tablets

5.22.1. Tablets such as iPads are powerful mobile computing devices, enhanced by a host of readily available applications (apps) developed by third parties. It is important to realise that these apps are not controlled by the NHS and that data moved, manipulated or stored using these apps may not be secure and may contravene UK legislations.

5.22.2. To comply with NHS Information Governance requirements great care must be taken if equipment is used with cloud services. Data governed by the Data



Protection Act must not be used or accessed via cloud services without permission from the Information Governance Team as this risks the data being stored outside of the European Economic Area.

5.22.3. If in doubt, disable the cloud services on your device will ensure data is not inadvertently transferred. Guidance on use of applications can also be provided by the IT Department.

5.23. Remote Working

5.23.1. Remote working applies to the use of the PRACTICE's systems and assets, such as laptops, tablets, mobile phones and also the use of personal, or other, computer equipment whenever work is undertaken away from PRACTICE premises.

5.23.2. Remote workers must:

- Password protect any work which relates to the PRACTICE's business so that no other person can access the work.
- Be positioned to ensure that work cannot be seen by any other person whom it does not concern.
- Take reasonable precautions to safeguard the security of the PRACTICE's equipment. This includes not leaving portable media unattended, including in the boot of a car, and keeping passwords secret.
- Inform the PRACTICE as soon as possible, if either the PRACTICE's equipment in their possession or any computer equipment on which work is undertaken, even if this is personal IT equipment, has been lost or stolen.
- Ensure that any work undertaken remotely is saved on the PRACTICE system or is transferred to the PRACTICE arrangements as soon as reasonably practicable.

6. Monitoring Compliance

6.1. The PRACTICE will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following method/s:

6.2. **IG Incidents** - Information Governance compliance will be monitored quarterly through the monitoring of reported IG incidents by the Practice Manager and Caldicott Guardian.

6.3. The DPO has responsibility for providing assurances that this policy is adequate for providing clear guidance in the event of significant changes which may affect it. The IG Lead will ensure that adequate arrangements

exist for:

- Reporting incidents and Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programs and progress reports
- Reporting Data Security & Protection Toolkit assessments and improvement plans
- Communicating IG developments.

6.4. **Privacy Impact Assessments** - Risks will be identified and monitored through the Privacy Impact Assessment process for all new and / or changed processes, systems and / or services.

6.5. In addition to the monitoring arrangements described above, the PRACTICE may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

7. Staff Training

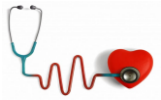
7.1. All staff (permanent, temporary, contract or seconded) likely to be in post for 3 months or longer, are required to complete the online mandatory IG training module- Data Security Awareness Level 1 within the first month of employment (or within two weeks of joining if they work with person identifiable information)

7.2. The Data Security Awareness Level 1 e-learning module can be accessed either through ESR (https://my.esr.nhs.uk/) or e-learning for health (https://www.e-lfh.org.uk/).

7.3. Further training is required for staff who process personal information, and staff within specific roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of the effective delivery of the training program.

8. Arrangements for Review

8.1. This policy will be reviewed no less frequently than every two years. An



earlier review will be carried out in the event of any relevant changes in legislation, national or local policy/guidance, organisational change or other circumstances which mean the policy needs to be reviewed.

8.2. If only minor changes are required, the sponsoring Committee has the authority to make these changes without referral to the Practice. If more significant or substantial changes are required, the policy will need to be ratified by the relevant committee before final approval by the Practice.

9. Associated Policies, Guidance and Documents

- Email and Internet Usage Policy 2023
- Data Protection and Confidentiality Policy 2023
- Records Management and Information Policy.
- Mobile and Remote Working Policy 2023.
- Staff Confidentiality Guidance 2023.
- Video Consultation Policy 2023.
- System Administration Policy 2023.
- Social Media Staff Use Policy 2023.

10. Equality Impact Assessment

The Equality Impact Assessment needs to be completed so that any decisions made are compliant with the aims of the Public Sector Equality Duty – and that any adverse impact for any protected characteristics are identified and resolved.

Bedford Street & Furzton Medical Centre

K82039

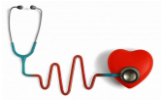
Appendix A

Equality Impact Assessment	
Does the scheme affect one of the following groups more or less favourably than another?	**If yes, explain impact and any valid legal and/or justifiable exception**
Age *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.*	No
Disability *Consider and detail (including the source of any evidence) on attitudinal, physical, and social barriers.*	No
Sex *Consider and detail (including the source of any evidence) on men and women (potential to link to carers below)*	No
Gender reassignment (including transgender) *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.*	No
Marriage and civil partnership *Consider and detail (including the source of any evidence) on people with different partnerships.*	No
Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements,*	No

K82039

part-time working, infant caring responsibilities.	
Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.*	No
Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.*	No
Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.*	No
Carers *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.*	NO
Other identified groups *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.*	No
Is the impact of the scheme likely to be negative? If so, can this be avoided? Can we reduce the impact by taking different action?	No – it is intended to have a positive impact on the lives of those involved and their families and carers – by ensuring appropriate iCT security

Bedford Street & Furzton Medical Centre



K82039

Appendix B

The NHSmail password policy was introduced in May 2019 to help keep the NHSmail service safe in line with the National Cyber Security Centre (NCSC) guidelines.

Passwords are valid for 365 days and all users will receive reminders to change their password via email 18, 10, 5, 2 and 1 day(s) before it's expiry date.

All passwords must follow the following criteria:

- They must be 10 characters or more in length without spaces;
- They must not match the previous 4 passwords used;
- Must not contain the users First Name or Last Name within the password;
- Not detected as a common password, for example Password123, Winter2018;
- Not detected as a breached password (a password used for an account that has previously been compromised or identified as having been breached according to an internet-based breach database).
- Please refer to the Application account guidance for more information regarding Application account password complexity requirements.

Important note

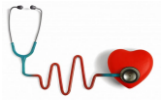
We know that common passwords are currently used on the NHSmail service by a number of users. In the future, users who do not meet the above criteria will receive a failure message when changing their password.

Top tip

A good way to create a strong and memorable password is to use three random words. Users should be creative and use words that are memorable to only them, so that people cannot guess their password.

NOTE:

Bedford Street & Furzton Medical Centre



K82039

Mobile numbers used to register for an NHSmail account must be based in the United Kingdom. Any NHSmail account registered with non-UK number will be disabled and will need to contact their local organisation to apply a UK based phone number to their NHSmail account. Please see Information – Non-UK registered Phone Numbers for more information.

Some reminders to help users keep their NHSmail account active and get the best experience from their account:

- **Record a UK mobile number and set a user account secret to their profile –** this will allow a user to reset their password via their local IT or NHSmail Helpdesk.
- **Register at least one authentication method on their account –** this will allow users to reset their password online at any time without contacting your local IT or NHSmail Helpdesk
-
- **Change password on all devices –** to prevent their account from becoming locked, users will need to update their password on all the devices (including personal devices) that they use to access NHSmail, for example mobile phone, Outlook desktop, tablet etc.

If you require additional help and support, the NHSmail helpdesk is available 24 hours-a-day, 7 days-a-week on 0333 200 1133 or by emailing helpdesk@nhs.net.

Last Reviewed Date	10/10//2024