Yewtree medical centre
21 Berryford Road, Liverpool, L14 4ED

Review Sheet

Last Reviewed 21 Jan '21	Last Amended 21 Jan '21	Next Planned Review in 12 months, or sooner as required.

Business impact	MEDIUM IMPACT Changes are important, but urgent implementation is not required, incorporate into your existing workflow.
Reason for this review	Scheduled review
Were changes made?	Yes
Summary:	This policy has been reviewed and updated with no significant changes. Use of the Confidentiality and Data Security Checklist, available in the QCS Resource Centre, will enable the Practice to provide assurances that measures are in place to ensure information is kept safe and secure, and handled, stored, and transmitted securely when in electronic form. References have been checked and updated.
Relevant legislation:	• Access to Medical Reports Act 1988 • Computer Misuse Act 1990 • Obscene Publications Act 1959 • Regulation of Investigatory Powers Act 2000 • Copyright, Designs and Patents Act 1988 • Electronic Communication Act 1990 • Equality Act 2010 • Freedom of Information Act 2000 • The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 • Human Rights Act 1998 • Access to Health Records Act 1990 • Data Protection Act 2018 • UK GDPR
Underpinning knowledge - What have we used to ensure that the policy is current:	• Author: Nursing and Midwifery Council, (2016), *Guidance on using social media responsibly*. [Online] Available from: https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/social-media-guidance.pdf [Accessed: 21/1/2021] • Author: Information Commissioners Office (ICO), (2018), *Health sector resources*. [Online] Available from: https://ico.org.uk/for-organisations/health-sector-resources/ [Accessed: 21/1/2021] • Author: ACAS, (2017), *Strategies for effectively managing email*. [Online] Available from: https://www.acas.org.uk/strategies-for-effectively-managing-email [Accessed: 21/1/2021] • Author: NHS Digital, (2020), *GP Systems of Choice*. [Online] Available from: https://digital.nhs.uk/services/gp-systems-of-choice [Accessed: 21/1/2021] • Author: NHS Digital, (2020), *The secure email standard*. [Online] Available from: https://digital.nhs.uk/services/nhsmail/the-secure-email-standard [Accessed: 21/1/2021] • Author: Department of Health, (2013), *Information: To Share or not to Share - Government response to the Caldicott Review*. [Online] Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_da-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF [Accessed: 21/1/2021]
Suggested action:	• Encourage sharing the policy through the use of the QCS App • Share ‘Key Facts’ with all staff • Ensure relevant staff are aware of the content of the whole policy

Equality Impact Assessment:	QCS have undertaken an equality analysis during the review of this policy. This statement is a written record that demonstrates that we have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by equality law.

1. Purpose

1.1 To set out the access requirements, operational standards and conduct expectations in respect of staff members using the computer hardware and software, the internet and NHSmail of Yewtree medical centre provided to support primary medical services delivery.

1.2 To support Yewtree medical centre in meeting the following Key Lines of Enquiry:

Key Question	Key Lines of Enquiry
CARING	HC3: How are people's privacy and dignity respected and promoted?
SAFE	HS3: Do staff have all the information they need to deliver safe care and treatment to people
WELL-LED	HW4: Are there clear responsibilities, roles and systems of accountability to support good governance and management?
WELL-LED	HW5: Are there clear and effective processes for managing risks, issues and performance?

1.3 To meet the legal requirements of the regulated activities that {Yewtree medical centre} is registered to provide:

- Access to Medical Reports Act 1988
- Computer Misuse Act 1990
- Obscene Publications Act 1959
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1988
- Electronic Communication Act 1990
- Equality Act 2010
- Freedom of Information Act 2000
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Human Rights Act 1998
- Access to Health Records Act 1990
- Data Protection Act 2018
- UK GDPR

2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following Patients may be affected by this policy:

- Patients

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

3. Objectives

3.1 All staff members, together with any others authorised to use the IT hardware and software at Yewtree medical centre for Patient care purposes (and has access to Yewtree medical centre information) understand their professional and personal data security and protection duties and information governance responsibilities.
3.2 All staff members comply with the policies, procedures and guidance of Yewtree medical centre and are appropriately qualified and trained in the safe, confidential and effective use of the computer system, personal computers and associated IT hardware, the internet and NHSmail email while at work.

4. Policy

4.1 Yewtree medical centre staff members and other users with formal computer access to the computer system, email and the internet must ensure that information remains confidential in accordance with Caldicott principles, the Data Protection Act 2018, the Freedom of Information Act 2000 and any other relevant UK legislation in force.
4.2 Yewtree medical centre provides the appropriate level of functional access to the computer system, NHSmail and the internet respectively, according to individual staff members' roles and responsibilities.
4.3 Individual staff members have their own unique passwords and login details for the computer system, the clinical system, NHSmail and any other NHS application that supports the electronic needs of Yewtree medical centre as a provider of primary medical services and NHS contractor. Passwords and login details must remain confidential and never be shared. Sharing passwords, login details or using another's password or login constitutes misconduct, unless authorised by The Operations manager for a specific purpose in unforeseen circumstances when a deadline must be met, such as data submissions e.g. CQRS.
4.4 Staff members must log off the network or lock their terminal and switch off the screen when leaving their desk to prevent anyone using that computer while the "owner" is logged in.
4.5 NHSmail and any messaging functions within the computer clinical system (e.g. electronic tasks) or add-ons (e.g. electronic document managers) are methods of communication. These are not records management systems. Where the content of emails or attachments, tasks or instant messages forms part of a record, the staff member/NHSmail user is responsible for adding the relevant information to that record whether it is in electronic format or hard copy.
4.6 The availability and variety of information available on the internet includes material that is reasonably considered to be offensive to others. The use of the internet to access and/or distribute any kind of offensive material and the deliberate accessing of offensive, obscene, indecent or illegal material from the internet (such as pornography, racist or sexist material, violent images, incitement to criminal behaviour or other unacceptable material), or matters not related to the business of Yewtree medical centre, will lead to disciplinary action which may lead to dismissal. Any act of misuse which compromises or potentially compromises the integrity of the computer hardware or software at Yewtree medical centre will be treated as gross misconduct.
4.7 Yewtree medical centre NHSmail is provided for secure practice business email. NHSmail is used to send Patient identifiable data to another NHSmail address securely. All NHSmail emails are business documents of Yewtree medical centre and may be accessed without the staff member’s permission for legitimate purposes, e.g. investigation of potential breaches of this policy or the Security Policy, or under any lawful circumstances. Only identified senior staff members are permitted to access another user's NHSmail. Staff members with data privacy concerns will raise these with the Data Protection Officer, Sophie Whittaker who can be contacted on Sophie.Whittaker@livgp.nhs.uk.
4.8 Computers and IT equipment, access to the internet and use of NHSmail are provided by Yewtree medical centre for business use by staff members during working hours only. Personal use of computers, the computer clinical system, NHSmail and internet access are not permitted.
4.9 Yewtree medical centre uses computers and a remote server to host the clinical system, NHSmail and the internet. To reduce the risk of hacking or contamination by computer virus, staff members will comply with procedures that keep the computer system safe and minimise risks to computer security.
4.10 Staff members at Yewtree medical centre do not send or encourage the receipt of libellous statements via its NHSmail, other email, or electronic communication media to avoid the risk of Yewtree medical centre incurring legal liability for damages as a result.
4.11 All NHSmail correspondence carries an approved NHS disclaimer at the bottom of the message

without exception. The content of this will change from time to time in accordance with the information governance requirements of the NHS Data Security and Protection Toolkit: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit.
4.12 Yewtree medical centre information is published with senior management approval and sign off only. All published information is accurate, up-to-date and kept under regular review for this purpose. Access to any online Yewtree medical centre publication rights are restricted to avoid reputational or commercial risk. Intellectual property rights and copyrights of any staff member, other person or organisation must not be compromised through any Yewtree medical centre internet publication.

5. Procedure

5.1 All NHS GP IT hardware and software is provided and maintained via locally commissioned providers. Hardware, NHS-specific and operational software is supported by the locally commissioned NHS GP IT service provider, while clinical software is hosted and supported by the selected GP clinical system supplier, e.g. EMIS or TPP. Each NHS GP IT provider/clinical system supplier has a helpline and is the first port of call for IT hardware and software issues that cannot be resolved in-house.

5.2 Use of NHS GP IT Hardware

- In the event that additional, non-NHS or standard operating software is required (e.g. for financial accounting), the introduction and downloading of active software must be authorised by the NHS GP IT provider only with the prior approval of The Operations manager
- There will be no unauthorised copying of data and/or removal of computer equipment/software
- Only encrypted USB data sticks authorised or supplied by the NHS GP IT provider or approved secure plug-in devices (e.g. printers, scanners) can be used with Yewtree medical centre NHS GP IT hardware

5.3 General Principles of Safe Computing in the Workplace

The NHS GP IT provider and the clinical system supplier respectively will ensure:

- A firewall is installed
- Antivirus software is installed and kept up to date
- Anti-spyware software is installed and kept up to date
- Regular backups are achieved
- IT support is in place in order to deal with queries and provide advice when using IT at work
- An overarching NHS GP IT/clinical system Business Continuity Plan is in place in the event of system failures

No-one authorised to use the computer system at Yewtree medical centre will be permitted to:

- Give out any email address unless the identity of the person/organisation asking for it and the purpose can be verified
- Open emails or attachments where the sender is not known, if it is suspected that the attachment is not what it seems or there is an NHS alert attached to the email or attachment
- Provide personal details unless the site being accessed for Yewtree medical centre business purposes can be fully trusted

5.4 NHSmail Message Standards

Any email sent from Yewtree medical centre must contain the following information :

- The sender's name, job title, practice address and direct or generic contact details, in an electronic signature in agreed standard format
- An NHSmail template disclaimer at the bottom of the message
- A request not to print the email in order to minimise waste and preserve resources for ecological purposes

and, if the Practice is a registered company, the:

- Full name of the company
- Registered number of the company
- Place of registration of the company

- Registered office address of the company (not a PO Box)

Emails are prone to misinterpretation according to the style in which they are written and presented. Care must be taken when writing content, especially if it sensitive, and it is wise to get someone more senior who is responsible and/or accountable to proofread to make sure the content conveys the message intended. Capitalising text within emails is to be avoided, as it implies the sender is 'shouting'. Staff members are expected to use the same degree of care and propriety and use professional language when emailing both internally and externally.

It is unacceptable and strictly contrary to Yewtree medical centre policy to use NHSmail to send jokes or messages of a personal, abusive, pornographic, offensive, sexual and/or racist nature - what may appear funny to one person may be regarded as offensive, distasteful or hurtful to others.

5.5 Use of NHSmail Expectations

NHSmail secure email system is provided for communication relating to the legitimate business of Yewtree medical centre. Staff members using NHSmail will do so in accordance with the following:

- It is a serious offence for anyone to send unsolicited commercial emails (spam) and text messages to individuals (including unincorporated bodies) who have not explicitly agreed to this in advance. Unless there is already an existing customer relationship with the individual, emails, text messages and other electronic marketing messages can only be sent to individuals with their explicit prior consent – i.e. an opt-in only
- All emails must comply with the communication standards of Yewtree medical centre as set out within this policy
- NHSmail messages and copies must only be sent to those intended and will be professional in content, while adhering at all times to the values of Yewtree medical centre
- NHSmail must not be used as a substitute for face-to-face communication or telephone contact
- If an email is confidential because it contains patient information, the user must ensure that the necessary steps are taken to protect confidentiality and only send to another NHSmail address with the **'.nhs.net'** extension as this is secure. Encryption or secure systems for identifiable data or confidential material are also permitted, provided the recipient can be verified and the system is password protected
- Yewtree medical centre will be liable for infringing copyright as well as for any defamatory information that is circulated either within the Practice or externally
- Offers or contracts transmitted by email are as legally binding on Yewtree medical centre as those sent on paper

5.6 Neither the NHS nor Yewtree medical centre permits the use of NHSmail for personal, unofficial or inappropriate purposes such as:

- Distributing offensive jokes
- Accessing or transmitting pornography
- Personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters)
- Online gambling
- Social networking
- Transmitting copyright information and/or any software available to the user
- Posting confidential information about any members of the team at Yewtree medical centre, Patients, commissioners, other providers etc.

Unauthorised personal, unofficial or inappropriate use of the email system is likely to result in disciplinary action and risks breaking the law.

5.7 Use of Web Browsers

The NHS GP IT provider authorises and makes available a browser type and version to support NHSmail, other NHS Digital applications and the clinical system. Web browsing is for research purposes only, personal use is prohibited.

Only reputable websites will be accessed using the computers of Yewtree medical centre to avoid the risk of malicious intrusion. Staff members are individually responsible for determining whether a website is safe and failure to take reasonable precautions may result in disciplinary action.

Registering on websites is often required to use the website for work purposes. Staff members are encouraged to do so and must ask their manager before doing this unless it is at the prior request of The Operations manager. The login and password details will be recorded in a confidential central log for business continuity purposes.

A staff member will be deemed to have committed gross misconduct if he or she uses unauthorised software, illegally copies software, gains unauthorised access to a computer or file on a computer or commits any other breach of data security rules laid down by statute or Yewtree medical centre. This will include (but is not limited to) sending offensive or inappropriate emails or accessing, downloading, viewing or distributing offensive, unsuitable, obscene or pornographic web pages or materials from the internet. Yewtree medical centre will notify the police where there are grounds to believe that a criminal act may have been or may be about to be committed.

5.8 Copyright

Under the Copyright, Designs and Patents Act 1988 copyright law can be infringed by making an electronic copy or making a ‘transient’ copy (which occurs when sending an email). Copyright infringement is becoming more commonplace as people forward text, graphics, audio and video clips by email. Therefore, staff members must not copy, forward or otherwise disseminate third-party work without the appropriate consent.

5.9 General Principles of Safe Internet and NHSmail Use in the Workplace

Yewtree medical centre will ensure that staff members:

- Have read and understood this policy
- Ensure NHSmail is configured to scan email attachments for viruses before opening
- Only address emails to people who really need to know about the subject
- Include a relevant title for each email message
- Ensure that they are aware of confidentiality and data sensitivity issues before sending messages
- Ensure that information published on a website is accurate and up to date before using it
- Not access websites that may contain inappropriate or offensive material
- Not download files or open email attachments unless they are certain the sender and the content are secure and can be trusted
- Not send large attachments to multiple recipients unless necessary
- Not send or forward junk mail, chain letters or virus warnings

5.10 Blogging and Social Networking

While Yewtree medical centre may use social networks for valid business purposes, staff members must refrain from any work-related conversations, "friending" Patients via social media or posting information about colleagues, Patients or Yewtree medical centre (in particular, defamatory information) on blogging or social networking sites at any time.

Participation in social media content that discriminates against any protected classification including age, race, religion, gender, national origin, disability, or genetic information, sexual preference and weight is included in the above. Evidence of such behaviour will be subject to disciplinary action.

5.11 Portable equipment

Portable equipment includes but is not limited to:

- Authorised USB memory stick/flash drives
- Authorised read-write compact discs/DVD/Zip drives
- Smartphones, laptops, iPads including tablets and cameras

Removable equipment must be stored securely at all times. It must be :

- Locked away when not in use
- Locked away outside working/operational hours
- Kept on the premises and not removed

Data within portable devices must be stored appropriately due to its potentially sensitive content.

5.12 Monitoring

For business reasons and in order to carry out the legal obligations of Yewtree medical centre, the professional and personal use of systems - including telephone and computer systems - may be continuously monitored by automated software or otherwise. Monitoring will only be carried out to the extent permitted or as required by law, and as necessary and justifiable for business purposes.

Yewtree medical centre reserves the right to retrieve the contents of NHSmail or other email messages, or to check internet usage (including pages visited and searches made) as is reasonably necessary for the interests of Yewtree medical centre, including for the following purposes (this list is not exclusive):

- To monitor whether the use of NHSmail or the internet is legitimate and in accordance with this policy
- To find lost messages or to retrieve messages lost due to a technical failure
- To assist in the investigation of any alleged wrongdoing
- To comply with any legal obligations

In order to inform external senders and recipients that NHSmail messages and emails sent by any staff member of Yewtree medical centre may be monitored, the following message must appear at the end of the email together with the email disclaimer:

"Under the Regulation of Investigatory Powers Act 2000, Yewtree medical centre regularly intercepts and monitors emails sent to it for the purpose of, for example, ensuring that only legitimate business is being carried on and to ensure the security of information being transmitted. Please note that when sending an email to any member of our staff, you accept that your email may be intercepted and/or read by other authorised members of staff."

5.13 Return of Equipment at Termination of Employment

When staff members leave their employment, Yewtree medical centre will require the return of all equipment (including SMART card, unless otherwise organised with the relevant registration authority team) on the last day of employment/service, or a P45 will be withheld until all equipment is returned.

5.14 Access to the Computer Clinical System and Use of Medical Records

Directly employed Practice staff members and attached community healthcare clinical staff (e.g. health visitor, community nurse, midwife) may have access to Patient information which is necessary for the effective care of the Patient, with their consent.

Access is at the discretion of senior management or identified individuals responsible for clinical care via the reception and administrative team. Patient records must not be removed from the premises of Yewtree medical centre, except where this is necessary for Patient consultations at branch surgeries, outlying clinics or in the Patient's home.

When transporting or using Patient records, they must be signed out if they are in paper format and remain in the personal custody of the user at all times (not left in a car or elsewhere unattended) and then returned to the premises of Yewtree medical centre and signed back in without delay.

Staff who remain Patients of Yewtree medical centre must not have access or attempt to gain access to their own medical records or those of friends, acquaintances or family members. Access to relevant computerised records will be barred and written records will be stored separately in a secure place. Access to a staff member's own records may only be granted under the terms of the Data Protection Act 2018, the Access to Health Records Act 1990 and the Access to Medical Reports Act 1988. Similarly, no member of staff is permitted to attempt to gain access to the medical records of their colleagues or members of their colleagues' families.

6. Definitions

6.1 Intellectual Property Rights

- Intellectual property rights refer to creations of the mind such as inventions, literary and artistic works and symbols, names and images used in commerce. These include patents and trademarks

6.2 Firewall

- A network computer system that monitors and controls all incoming and outgoing data using pre-set security rules

6.3 Antivirus Software

- This is a computer term for software that has the ability to prevent, detect and remove malicious items. It may also be known as Anti-Malware Software

6.4 GPSoC

- GP Systems of Choice (GPSoC) was a contractual framework to supply IT systems and services to GP practices and associated organisations in England. The GPSoC Framework ended on 31st March 2018 when a continuity agreement was agreed to ensure that the essential core services from GPSoC remain available until a replacement GP IT Framework is in place. The GPSoC Continuity period may run until 31st December 2019
- GP practices can choose systems that best suit their needs from a range of four principal system suppliers. These are TPP SystmOne, EMIS Web, InPS Vision and Microtest Evolution. This means Practices get a choice of approved systems and save time by not having to run their own procurement. They benefit from discounts through the central purchase and standardised terms and conditions

6.5 NHSmail

- NHSmail is a secure email system that must be operated and used in accordance with a set of clear policies and procedures. NHSmail is available to organisations with a valid reason to use it

6.6 GP Clinical System

- A digital clinical system supplied for General Practices by the NHS to hold and provide access to the electronic medical records of registered patients. It is generally hosted by the supplier and supports joined-up working across the healthcare system. The use of a clinical system helps healthcare professionals make informed clinical decisions with the help of an integrated evidence base and record them using nationally used clinical codes

6.7 Encryption

- The process of converting information into a form unintelligible to anyone except holders of a specific key or password.

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- General practice requires NHS-supplied and supported IT hardware and software to provide safe evidence-based primary medical services (this includes virus protection and back up functions for the computer system)
- Yewtree medical centre may require additional non-NHS software to support business processes and this must be approved by the local NHS GP IT provider before purchase and installation
- The computer system of Yewtree medical centre provides access to medical records, NHSmail and the internet for Practice use only and any misuse, criminal act or anything that puts Yewtree medical centre at any kind of risk will be dealt with in the appropriate manner
- Yewtree medical centre staff members have the appropriate level of access to the computer system in order to carry out their duties and responsibilities - this may be extended to community healthcare staff as members of the wider multidisciplinary team involved in Patient care with individual Patient consent
- Yewtree medical centre is entitled to monitor and record staff members' NHSmail and internet use in the Practice to ensure all systems are being used for legitimate business purposes (no criminal acts or policy breaches are taking place and no illegal software has been downloaded), or to check emails during absence
- The computer system is for Practice business only which excludes any personal use or any content that could be deemed as offensive, distasteful or hurtful to others. The same degree of care and propriety must be taken when sending emails both internally as well as externally

Key Facts - People affected by the service

People affected by this service should be aware of the following:

- Yewtree medical centre requires a computer system to gather and store electronic data in your medical records, which is used to provide safe care to you in a secure and confidential manner, based on the most up-to-date information about you and evidence-based guidelines
- Members of the Practice Team with access to your electronic medical records (with appropriate level access for their role) are granted this formally according to NHS Digital and clinical supplier policies
- The data held in your medical records, and anywhere on the Practice computer system, will only be shared with your consent unless there is a valid reason for this to be otherwise (e.g. police investigating a crime), at which point an assessment will be made by the responsible senior member of the Practice Team whether that data can be shared
- Staff members are authorised to only use the computer system, NHSmail or the internet to access your records, look at your data, contact you, or otherwise access your data for valid Practice purposes

Further Reading

As well as the information in the 'underpinning knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

NHS Employers: New to the NHS? Your guide to using social media in the NHS:
https://www.nhsemployers.org/~/media/Employers/Publications/NOVEMBER%20Your%20guide%20to%20using%20social%20media%20in%20the%20NHS.pdf
NHS Digital - NHSmail policies:
https://digital.nhs.uk/services/nhsmail/nhsmail-policies
NHS Data Security and Protection Toolkit:
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit

Outstanding Practice

To be ‘ outstanding ’ in this policy area you could provide evidence that:

- There is an innovative use of technology to improve communication and to minimise the risk of missed referrals, discharge information, tests and results etc; to remind patients about referrals and tests for their health and to preserve NHS resources
- Clinical software and communications technology are used to support vulnerable patients and those with complex medical needs or with long-term medical conditions e.g. via a secure multidisciplinary team prompt system
- There are fast and secure arrangements in place for the secure and confidential exchange of information with community and secondary care services and departments, to avoid the need for Patients to attend one or more appointments
- Using social media to improve health outcomes by reaching a wider Patient audience that is usually hard to reach e.g. teenagers and working-age males
- All practice staff members are trained to be confident and competent in the safe and legal use of IT, the internet, NHSmail and social media so that Patient for improved outcomes and the best possible Patient experience minimising risk and maximising the use of available resources by shortening pathways using communication technology
- The wide understanding of the policy is enabled by proactive use of the QCS App
- Yewtree medical centre is and chooses to be at the forefront of communications technology and NHS information technology developments, as early adopters who are able to assist other practices and so improve the effectiveness and safety of the primary medical services that Patients receive

Forms

Currently there is no form attached to this policy.