NHS
The Royal Orthopaedic Hospital
NHS Foundation Trust

ACCEPTABLE USE STANDARD FOR IT SYSTEMS AND EQUIPMENT

Content

ACCEPTABLE USE STANDARD FOR IT SYSTEMS AND EQUIPMENT

NHS
The Royal Orthopaedic Hospital
NHS Foundation Trust

Introduction

This document sets out the minimum standard of acceptable use of Trust IT systems and equipment to ensure you keep information safe, secure and confidential.

Please read this as you need to understand your responsibilities. A breach of, or refusal to comply with, this standard is a disciplinary offence which may lead to disciplinary action being taken in accordance with the Trust's disciplinary policy. Where appropriate serious incidents may even be referred to the Police for formal criminal investigation.

It is your responsibility to use Trust IT equipment, software and systems correctly to keep information confidential and safe:

- It's the Law - UK Data Protection Act 2018
- It's in your contract terms and conditions
- Clinical staff – It's in your professional codes of conduct.

Relevant policies:

- Information Security Policy
- Information Governance Policy
- NHSMail Acceptable Use Policy

This standard applies to all employees of the Trust, including permanent, contract and agency staff and any other person granted access to the Trust's systems and intranet.

Misuse of IT

Do not use systems, the internet or email for malicious purposes – this is a disciplinary offence. This includes, but is not limited to:

- Acquiring or sending content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene.
- Acquiring or sending offensive or criminal material
- Distributing statements of a political, religious or personal nature
- Deliberate copyright or intellectual property rights violations
- Downloading, storing or transmitting large volume of data for personal use
- Using NHS information systems or data for personal gain or for profit
- Trying to hack systems or deliberately putting spyware, viruses or other malicious software into the network or system.

ACCEPTABLE USE STANDARD FOR IT SYSTEMS AND EQUIPMENT

NHS
The Royal Orthopaedic Hospital
NHS Foundation Trust

IT Equipment and Systems/Software

All IT equipment (including smart medical devices) and software/systems must be assessed, approved and signed off by the IT Department (and Information Governance where they hold identifiable data). Don't buy equipment or software without approval as this could be incompatible with the Trust infrastructure or be unsafe and therefore unusable. This includes items purchased with charitable funds, donated equipment, devices used for trials or items on loan.
Do not install your own software on trust devices
All IT equipment belongs to the Trust and must be returned to the IT Department if you no longer need it or are leaving the Trust. Do not pass it on to a colleague unless you tell the IT Department, and they authorise it.

The Trust reserves the right to audit and inspect Trust IT equipment given to you including checking the software that is loaded and/or data held.

Using mobile devices e.g laptops, tablets, smartphones

It is your responsibility to take care of Trust owned devices:

- Keep your device with you or lock it away when not being used.
- Keep your device out of sight when travelling in a car and don't leave it in the boot of a car
- If you take your device on a flight, keep it with you as hand luggage
- Carry devices in an anonymous bag
- Don't keep your usernames and passwords with the device
- Trust devices are for work purposes only. Don't share your device with family or friends.

If your device is damaged or stolen, report this to your line manager and IT Department immediately.

Removeable media

If there is a genuine business need for a removable device e.g. camera you must get this issued and approved by the IT Department and the device must be encrypted.

You will not be issued with hard drives or USB data sticks to transfer data.

ACCEPTABLE USE STANDARD FOR IT SYSTEMS AND EQUIPMENT

NHS
The Royal Orthopaedic Hospital
NHS Foundation Trust

Using your own devices and software

- Don't use your own personal devices to store Trust information.
- Don't connect your own devices to trust systems or equipment
- Don't store Trust information on public Clouds
- Don't use Apps on personal devices to carry out Trust business unless they have been approved by the Trust.
- Don't use WhatsApp to discuss patient information unless it's an absolute emergency or you don't use identifying information

You can put NHSmail onto your personal smartphone/tablet. Please note - If your device is lost or stolen, you must notify the IT Department and they will most likely need to remotely wipe NHSmail and its contents which would also wipe out all other data on your phone including photos. So, if you do use NHSmail on your on device, please make sure you back up your personal content, in particular your photos.

Access, locking, passwords and information storage

Your access to systems is restricted to what you need to do your job. Your access can be audited to make sure you only look at information in these systems relevant to your job. Accessing patient data of someone you are not caring for is a disciplinary offence as is accessing colleague's information inappropriately.

Don't use IT systems unless you have had appropriate training.

If you leave your system unattended lock the screen or log off.

Keep your password secret and don't share it. We advise you to make your password difficult to crack e.g. combine three random words to create a single password (Applenemobiro1!)

Don't store information on the hard drives of PCs, laptops or other mobile devices. Data must be kept on the relevant system.

Using Email

You are given an NHSmail email account which is the Trust's standard method for communication. You must always use this for Trust business, particularly when you are emailing personal and sensitive information e.g. about staff or patients. As well as not misusing email described above:

- Never use your own personal email accounts for Trust business
- Don't email Trust information to a personal email account. In particular, never email patient information or confidential staff information.
- Don't open emails if you don't recognise who they are from
- Don't click on links in the emails unless you are absolutely sure they are valid

If you write about staff or patient in emails, they are entitled under data protection legislation to see that information so be professional and accurate about what you say as your email could end up in a law court or employment tribunal.

The email system is not a records management system – it's for communication. Manage your inbox and either file your emails under appropriate headings or delete them.

Don't use the email system to store attachments. If you need to keep an attachment, copy it to an appropriate folder on OneDrive or SharePoint and then delete it off the email.

Information held or passing through the email system is the property of the Trust. Your emails are not routinely monitored but the Trust reserves the right to access, read, print or delete emails at any time.

Using the Internet

You can you use the Trust internet for personal use but only during your breaks. The Trust blocks illegal and inappropriate sites and you won't be able to access social media or chat rooms. Your manager can ask for a report on your usage and you can be disciplined for using it for personal use during work time and for unacceptable use. If you need access to a website that is blocked for business use, contact the IT Service Desk to request a site be unblocked.

Social Media

Be careful what you say on your own social networking sites. You can talk about the Trust but if you post rude or offensive statements about patients or colleagues or bring the Trust into disrepute, this is misconduct and disciplinary action could be taken. Also, action will be taken in cases which involve discrimination, victimisation or harassment. If you have an issue with the trust, deal with it using the Trust's procedures and policies.

Incidents

Please report incidents where IT systems or services have been misused either by accident or on purpose – including near misses. Use the Ulysses system on the intranet or tell your line manager or IG Manager. This will help us learn why incidents happen and stop them happening again.

Using OneDrive and SharePoint

OneDrive is your own personal folder. Keep things like your PDR, payslips, training materials etc. Do not keep information that you need to share with colleagues on your OneDrive. This must go into your department's SharePoint.

SharePoint is for corporate and business records. Do not use it to keep patient records that are part of a health record e.g. letter, image, results. These must be kept on the relevant patient system or on the casenotes. You can keep admin type patient records e.g. trackers, spreadsheets.

NHS
The Royal
Orthopaedic Hospital
NHS Foundation Trust