Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Policy
Code: IM1
Issue number: 7

Information Communications Technology (ICT) Acceptable Usage Policy (AUP)

Lead executive	Director of Operations
Authors details	Head of ICT Services 0300 303 8182

Type of document	Policy
Target audience	All CWP and partner organisation employees, contractors (also responsible for sub-contractors)
Document purpose	Determining what is deemed to be acceptable use of CWP's Information Communications Technology services

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 11th Oct 21
Implementation date	Oct 2021	

CWP documents to be read in conjunction with	
GR3	Risk management Policy
IM7	Code of Confidentiality Policy
GR12	Media Policy
IM6	Information Sharing Policy
GR17	Freedom of Information Act Policy
IM10	Information governance policy
HR13	Registration authority policy
HR3.3	Disciplinary policy and procedure
GR41	Corporate records policy
IM5	Information asset register policy
CP3	Health records policy
IM2	Email management procedure
CG2	Mobile devices policy
CG1	Fraud theft and corruption policy

Document change history	
What is different?	Specific guidance on Office365 applications added. Additional guidance on request process for new technologies Syncing trust data to personal devices is not permitted
Appendices / electronic forms	*N/A*
What is the impact of change?	

Training requirements	Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation

Clinical Services	*Clinical Services representatives of IG & DP Sub-Committee*
Corporate services	*Corporate services representatives of IG & DP Sub-Committee*
External agencies	*Not applicable*

Financial resource implications	*HEI PROVIDERS*

External references
1. None

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable? Not applicable		
Is the impact of the document likely to be negative? - If so, can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	Not applicable	

Contents

Glossary

Data – any documents, files or information

Device – Desktop computer, Laptop, Tablet or mobile/smart phone

Mobile phone – portable phone enabled by a sim card as distinct from a cordless phone, which are an extension of a phone physically connected to a landline.

Smart phone - a mobile phone that is capable of sending/receiving data and accessing applications.

Microsoft Office – suite of software installed as standard on all CWP computers containing Word, Excel and Outlook, plus Teams. The new version is Office365.

Microsoft 365 – Microsoft 365 (M365) is the new name for Microsoft Office365 (O365) for ease of understanding we will refer to Microsoft Office in this document.

N365 –the shared NHS platform that hosts Microsoft Office, used by CWP and managed by NHS Digital.

Microsoft Teams – Microsoft Teams is an O365 application that enables users to send instant messages, make internal calls, share, edit and collaborate on files in a central location.

Microsoft Forms – An O365 application that allows creation of Surveys and quizzes.

1. Purpose

The purpose of this policy is to outline the acceptable usage of the Information Communications Technology (ICT) resources within Cheshire and Wirral Partnership NHS Foundation trust (CWP). These rules are in place to protect the employee and CWP. Inappropriate use exposes the trust to risks including loss of data or access to clinical systems, potential legal proceedings, reputational damage and substantial fines.

2. Scope

This policy applies at all CWP employees, contractors, bank staff and anyone accessing CWP systems from third party companies. It also covers any device that can connect to the CWP infrastructure.

3. User Identity

To access the trust network, each member of staff is assigned a user account, together with an initial password which users are forced to change at first logon. The line manager is responsible for requesting the user account in good time for it to be available on the new employees starting date.

The user account uniquely identifies each user and is in effect a digital signature when accessing all resources on the network including email, internet, shared drives and key applications.

All access is logged against each individual user account. It is therefore the responsibility of each user to ensure that they don't share or divulge their password to anyone else. Staff should never write their user account or password details down.

When logging on to the CWP network each user is agreeing to abide by this policy.

4. Sanctions

Failure to comply with this policy can result in sanctions managed via the trust disciplinary procedures which may result in dismissal.

5. Monitoring

In order to ensure compliance with this policy, all employees should be aware that email and Internet usage is monitored to ensure compliance with legislation and policy by the ICT Services, reports are available to HR and line managers.

6. Agreement

All trust employees, students, contractors or temporary staff who have been granted the right to use the trust's ICT Infrastructure by their line manager, are required to acknowledge this agreement by confirming their understanding and acceptance of this policy. Acceptance is completed when logging in to the computer and clicking OK.

Higher Education Institutions wishing for students to be able to use CWP Education Laptops during placement with CWP accept that should a student be found to contravene elements of this policy appropriate disciplinary action will be taken. The HEI agrees to financially compensate CWP for any damage or loss of/to equipment by student. By signing the laptop use agreement form (provided at placement) and by signing onto CWP ICT systems, the student is accepting that they will adhere to this policy.

7. Breaches of this policy

All breaches of this policy should be logged with the trust incident management system (Datix) and consideration should be made as to whether People Services should be contacted to discuss possible disciplinary steps.

No action should be taken by users or managers in respect of any ICT equipment identified as possibly being involved with a breach of this policy, as this could impact digital forensic investigation. A call should be logged with the ICT Service Desk and appropriate action will be taken by ICT Services to secure the relevant ICT equipment.

8. Access control to ICT equipment and passwords

Only devices that are owned by CWP and managed by ICT Services can be connected to the CWP network. CWP data should not be downloaded or saved to a personally owned device. There is an increased risk that information could be visible to family members or close contacts and a data breach could ocurr.

Access permissions to the network will be allocated on the requirements of the user's job, rather than on a status basis.

The request for a new user account will need to be raised by the employee’s line manager, to the ICT Service Desk.

Staff are responsible for ensuring their password is kept secure and therefore should not be written down.

The password is required to be:

- A minimum of 10 characters in length
- It is recommended that staff use 3 random words to make a password that will be memorable and difficult to compromise, it’s recommended that special characters are used
- Should not contain parts of their username
- Will expire annually and will prompt you to change it
- Must be different to the last 4 passwords used

It is the responsibility of the line manager to inform the ICT Service Desk of any leavers, moves or changes to staff.

9. General use and ownership

Information contained on portable computers is especially vulnerable, special care should be exercised and this type of device should never be left unattended in a public area.
Users are required to “lock” unattended PCs, laptops and tablets, if they are away from the desk. On Windows devices, this achieved by pressing the CTRL-ALT-DEL keys at the same time and selecting lock this computer.

PC's, laptops and tablets will automatically be locked after 10 minutes of inactivity.

Personalised screensavers are not permitted on trust devices or as backgrounds on video conferencing platforms.

Users are advised that the data, files or emails they create on any CWP system, remain the property of CWP.

ICT Services will audit networks and systems on a periodic basis to ensure compliance with this policy.

10. Security and proprietary information

Information contained on all trust systems should be classified e.g. NHS confidential, NHS protect, as defined by corporate records policy. Examples of confidential information include but are not limited to: corporate strategies, research data, and patient confidential information. Employees should take all necessary steps to prevent unauthorised access to this information.

Permissions to Outlook Calendar are set appropriately but are potentially viewable by all staff. Users who use diary systems e.g. Outlook Calendar, and enter personal identifiable data (PID) in to those systems, need to ensure that access permissions to those diaries are set so that only permitted staff have access to those details.

Storage of user files

User files must be stored in an appropriate network location this could be a network file share or folder or home drive (Z drive) and should not be stored on the local C drive or desktop of a PC or laptop.

This is to avoid any kind of data loss as local C drives and files saved to the desktop are not backed up and therefore cannot be restored to the current or previous version of the file.

It is a mandatory requirement that all trust PC's, laptops and tablets are configured to automatically:

- Apply operating system and application security updates, which have been approved by ICT Services.
- Apply Anti-Virus updates.

Users should make no attempt to disable these systems, as they could put the whole CWP network at risk and which could mean that systems are not accessible or a data leak could occur.

Users of laptops and tablet devices must connect their device regularly to the trust network to ensure the latest operating system patches and anti-virus updates are applied. This needs to be done at a minimum of every 30 days. Time should be put aside to allow updates to be downloaded and implemented.

Downloading or syncing any CWP data to personally owned devices via the internet is also not permitted including documents via Office365, Teams or Email.

Should a Virus alert be displayed on the screen of PC, laptop and tablet device, users should contact the ICT Service Desk immediately.

11. Unauthorised Applications / Software

Only applications/software approved by ICT Services can be installed on trust owned PC's, laptops and tablet devices. This includes free software or services available via the internet.

Under no circumstances should staff attempt to install software without clearance from the ICT Services. All requests for new applications or software must be submitted to the ICT Service Desk and allow time for any technical and governance processes to be undertaken.

Users wishing to purchase non-standard hardware or software , any requirement not met with the catalogue requires the staff to contact ICT Services to discuss their requirements and complete an assessment where necessary prior to any purchase or sign up to a service.
Where new technologiesare being implemented, the nature, scope, context and purposes of processing of information should be taken into account, if likely to result in a high risk to the rights and freedoms of the data subject, a data protection impact assessment must be completed to assess the risks and impact of the envisaged processing on the protection of personal data. A template for completing a
Data Protection Impact Assessment may be found on the trust's information governance page of the intranet. Where the trust cannot mitigate against significant risks, the trust will be obliged to consult with the Information Commissioner's office prior to any processing of data.

12. Electronic communication acceptable usage

The trust recognises the importance of electronic communication in a safe and secure environment in compliance with data protection, legal and confidentiality laws and regulations.

12.1. Privacy

The trust respects an individual's right to privacy with regards to personal emails. However, the trust does not recognise privacy concerns relating to emails used for business or clinical purposes. This is necessary as the trust reserves the right to ensure compliance with this policy by audits of electronic mail usage and content.

12.2. Confidentiality

Consider how you plan to share data to ensure compliance with the confidentiality policy. Patient Identifiable, sensitive or confidential information should not be shared via Microsoft Teams or Microsoft Forms. Patient information should be stored by default as part of the clinical record.

Emails containing Person Identifiable Data (PID) can be sent to other bona fide NHS email addresses, usually of the format:

- firstname.surname@trustname.nhs.uk
- name@NHS.net

Emails containing PID that require to be sent to non NHS third parties, are required to be sent via the NHSMail email encryption service, details of which can found on the ICT section of the Intranet.

12.3. Professional conduct

Users of ICT systems whether internal or external to the trust are expected to conduct their activities in a professional manner.

Electronic communication, used for business and clinical purposes, must be treated the same way as formal business correspondence. Therefore, staff should identify themselves appropriately. For example give your name, job title and department in an internal email but in also include your address for a external email. . Although there is no legal requirement to include this information, it is sensible and courteous to explicitly state to the recipient who the sender is.

Content

Users are prohibited from sending communications in any electronic format that may be deemed as:

- Defamatory
- Abusive
- Sexist
- Racist
- Pornographic
- Unsolicited mail i.e. SPAM, chain letters, bulk mailings

The email systems should only be used for business relating to the trust, except for the occasional personal use. If necessary please clarify what is deemed acceptable with your line manager.

Users should not use it for any commercial or illegal activities.

Forwarding emails

Staff are not permitted to set auto forward rules on their mailboxes to any destination outside of CWP as this can result in data being sent insecurely and potential breaches of Data Protection legislation.

Computer viruses

Any mail message received by an electronic mail user has the potential to be infected with a computer virus. The trust protects its email system with virus checking software, which will identify a computer virus within an email at the point of entry to the trust.

Deletion of electronic communications

Users are advised that the deletion of an electronic message, whether email or chat does not guarantee that the message has been permanently erased. For the purposes of this policy, users need to be aware that a permanent record of their deleted messages may exist.

Unsolicited emails

Users should be aware of certain types of unsolicited email, sometimes known “fishing / phishing emails”, that pretend to be from trusted sender, eg “IT Department” or financial institution and ask the recipient to send their username and password. On no account should that information be given. Staff should contact the ICT Service Desk to alert of them incident.

Statements of facts untrue

Statements of untrue facts, which damage the reputation of the person or company or hold him/her up to hatred, ridicule or contempt, are libellous. If expressing an opinion via any form of electronic message you must ensure that the relevant facts are set out.

If a breach of security is recorded under your login the burden of proof will be with you to show that you are not responsible for the breach.

13. Office365

Microsoft Teams

Recording any clinical or confidential meetings via Microsoft Teams recording function is not permitted for the following reasons:

- At present there is no process available for storage or retention of this type of data in CWP clinical systems
- Possible need to disclose recordings in response to a Freedom of Information Request (FOI) or Subject Access Request (SAR) and potential need to redact/blur parts of a recording

Live transcriptions of any clinical or confidential meetings held via Microsoft Teams are not permitted for the same reasons.

Microsoft Forms

When creating or responding to surveys, quizzes or polls in Microsoft Forms be aware of the following:

- Do not use Forms to collect patient identifiable, sensitive or confidential information.
- Be clear with respondents about whether the survey is anonymous. Internal staff names and email addresses are captured in the background unless specifically set to anonymous.

14. Internet acceptable usage

Monitoring usage

All outbound Internet traffic passes through a web filter system, which captures each website request made be each user. The web filter is also used to block certain websites as they are deemed inappropriate for viewing within the workplace or have limited bandwidth assigned to them to deter abuse e.g. gambling sites.

Responsibilities of the user

It is the responsibility of all staff within the trust to ensure that computer systems and the data, which is accessed through them, are safe and secure.

Permissible access

All staff have access to the Internet via computers located throughout the various trust premises. This access is primarily for Healthcare related purposes, which includes professional development and training.

In line with the spirit of this policy staff may use the trust internet service for reasonable, personal use on their own time, subject to compliance with this policy and authority from their line manager. Queries concerning the definition of reasonable, personal access should be directed to the individual's line manager.

Non-permissible access

Offensive material includes hostile text or images relating to:

- gender,
- ethnicity,
- race,
- sex,
- sexual orientation,
- religious or political convictions
- disability.

Access to gambling sites is also prohibited. This above list is not exhaustive and should a user be uncertain as to whether a subject could be deemed offensive, they should contact their line manager.

Other than instances which demand criminal prosecution, the trust is the final arbiter, that is the trust will have the final decision on what is or is not offensive material, or what is or is not permissible access to the Internet. See HR 3.3 Disciplinary policy and procedure.

Unintentional breaches of security

If you unintentionally find yourself connected to a site which contains sexually explicit or otherwise offensive material you must disconnect from the site immediately and inform your line manager.

This is expected to be recorded for audit purposes to ensure compliance with this policy.

Downloading files

The trust does not recognise the Internet as a primary source and/or a preferred method of software acquisition. Consequently there is no requirement for staff to download any software directly from the Internet. If a member of staff believes they have a valid business application that can be sourced via the Internet then the software purchasing process via the ICT Service Desk must be followed.

To intentionally introduce files which cause computer problems could be prosecutable under the Misuse of Computers Act (1990).

Social Media

The trust has a corporate presence on a number of social media platforms including but not limited to; Facebook, Twitter and You Tube. All staff are responsible for maintaining a positive reputation on behalf of the trust with regards to any utilisation of these tools. Therefore staff who wish to utilise such tools extensively for the purpose of sharing information in a professional capacity should seek advice from the Communications Team before doing so. The Communications Team is available to support and give guidance on any communication and/or engagement tools. Further information and guidance on social media can be found within the Communications Strategy or by contacting the Communications Team directly.

WhatsApp

WhatsApp is approved for use as it can be useful to support business continuity plans especially in the event of an outage of other standard communication systems. Personally identifiable or sensitive data should never be shared via the WhatsApp platform.

Confidentiality

You are bound by the confidentiality and security policy of the trust, and by the common law duty to maintain confidentiality concerning the data and information you use as part of your everyday work. Under the Data Protection Act you may not disclose any Person Identifiable Data (PID). Furthermore, you may not disclose confidential information relating to any aspect of the business of the trust.

15. Usage of Laptops, tablets and mobile phones

Data Protection and Caldicott

In all cases where data is stored on portable ICT equipment and media, encryption of the data is mandatory and any breach must be reported via the trust’s Information Governance Incident Reporting procedure.

Storage of classified data, including Person Identifiable Data (PID)

Encrypted equipment and media can be used to store these types of information for work related purposes only and its is the responsibility of the equipment and media owner to ensure adequate physical security measures are in place and files are protected by passwords:

- minimum length of 10 characters
- combinations of letters and numbers (do not use obvious combinations e.g. abcd or 1234 etc)

This is to safeguard against unauthorised access or loss of the equipment or media.

Transfer of this type of data to other organisations via media, for NHS purposes, is also permitted, as long as the same precautions detailed above are followed.

Storage of non-classified data

Equipment and media can be used to store data of this type and an appropriate level of physical security must adopted by the media owner. See corporate records policy for classification descriptions.

Transportation of equipment and media

Approval to transfer confidential or sensitive information to removable media must be obtained by line manager. To enable the transfer the line manager will need to contact the ICT Service Desk. It is the responsibility of the line manager to check that only the relevant information is transferred. In the case of media, the owner should ensure that appropriate transportation methods are in place relative to the classification of data stored on the media.

Where media is transported, either by a third party or another trust department, physical safekeeping of both the media and the data contained therein must be assured. It is the responsibility of the owner to maintain an accurate written account of the transportation of the media, which will be subject to audit.

Mobile phone usage

CWP has a zero-tolerance policy for texting while driving and only hands-free talking while driving is permitted.

Private usage, defined as any communication made (or accepted reverse charge calls), including voice, text messages, web services, premium rate services and anything else which is not wholly, exclusively and necessary in the performance of the users trust duties.This could result in any cost to the trust being reclaimed from the individual.

The trust reserves the right to monitor and log mobile phone use and content, and to access and report on this information which includes private and personal use. Monitoring may lead to a formal investigation if a serious breach is suspected; this may then lead to disciplinary action.

Internet access via non-CWP networks

Using CWP portable equipment to access the Internet / trust systems via partner organisation networks e.g. NHS organisations or local government, is permissible, subject to the use of the trust’s secure remote access service and conformance to the trust’s Internet usage policy.

Using CWP portable equipment to access the Internet / trust systems via public networks is not currently permissible, as it is insecure.

Physical security

The following security precautions should always be followed when using equipment and media;

- Laptops should be secured to a desk or other appropriate point if left unattended during working hours, within the trust, using an approved security cable.
- At the end of working hours, laptops and tablets, should placed in secure local location e.g.; desk drawer.
- When off site equipment must not be left unattended.
- All media should be removed from equipment and stored in a secure location;
- When travelling and not in use ensure equipment and media are stored securely out of sight in the car, however, if it is considered that it would be safer from a theft and / or risk management point-of-view to take the equipment in to the building, then these should be taken in and should not be left unattended at any time;
- If you choose to use equipment in public places or at home be aware that it's likely you will draw attention of those people around you so ensure that information on the screen cannot be viewed by others which could lead to unauthorised disclosure of the information being processed.

16. Third Party Access

Third party access to the network such as suppliers, contractors or anyone external to CWP will be based on a formal support contracts that satisfies all necessary NHS security conditions and should be carried out remotely or via CWP devices.

ICT Equipment

Third parties are not currently authorised to use their own ICT equipment to connect to the trust's ICT network.

Media

Any third party wishing to use removable computer media within the trust for work related purposes, such as presentations, is only authorised to use this media in non-networked Trust personal computers. It is the responsibility of the owner of the non-networked PC to ensure the PC is safe to use after the media has been physically removed from the computer.

17*.* Safe disposal of ICT equipment and media

To dispose of ICT equipment containing a hard disk drive, a Service Request should be logged with the ICT Service Desk, who will arrange for safe disposal. In the case of media when it's no longer required, it must be physically destroyed to prevent any subsequent data access. Any other ICT media such as floppy discs, CD ROMs, and DVD's should also be returned to the ICT Service Desk for shredding.

Please be aware when reusing media, deletion of data doesn't actually remove the information from the media and it can be recovered. Consequently, under no circumstances should media be sold on or given to a third party. For guidance on re-using removable computer media please contact the ICT Service Desk for further information

18. Incident reporting

In the event of loss of equipment or media must, it must be reported to:

- Your line manager or their deputy
- ICT Service Desk - so that any containment action can be taken accordingly
- Logged as incident on the trust incident management system (Datix)
- The trust's Lead for Information Governance
- In the event of equipment loss / theft, this should also be reported to the relevant Police Service. See CG1 Fraud, theft and corruption policy

19. Responsibilities of ICT Services

NHS statement of compliance

ICT Services staff are delegated agents of the Chief Executive are responsible for maintaining a safe and secure computing environment in the trust.
To enable ICT Services staff to fulfil their duties they are given elevated system privileges, by logging in to their privileged account they accept that their actions are monitored and they are accountable to the highest standards of use.

Monitoring and blocking internet access

ICT Services provide a facility for monitoring and blocking access to inappropriate websites.

Should a Manager have a concern about an individual's use of the Internet, ICT Services can provide a log file which will contain details of the site accessed by the user, the time of day the sites were accessed and for how long. The Manager should seek advice from People Services before contacting ICT to ensure that all relevant HR policies and procedures are being followed correctly.
An email should be sent to the ICT Service Desk requesting the report to be created by the server team, but the name of the staff member should not be put on the request.
The HR representative should contact the Head of ICT Services with the name and the call reference number.

Network username and password management

ICT are responsible for managing username and password, this includes:

- Setting up new users in accordance with the agreed naming convention;
- Issuing passwords;
- Deleting expired accounts;
- Disabling dormant accounts;
- Removing access rights when staff leave the trust, when informed by HR;
- Undertaking regular audits to support these functions.

Security patch management

ICT Services will ensure that devices that are connected to the network have appropriate security patches updated/applied as required, including:

- Operating system patches
- Application security patches
- Anti-Virus updates

Breaches of the policy

ICT will undertake appropriate investigations on any breach of this policy and undertake actions to ensure the integrity of any ICT equipment suspected of being used in the breach of the policy, to allow possible forensic examination.

Maintenance contracts

ICT Services will ensure that maintenance contracts are maintained and periodically reviewed for all ICT infrastructure equipment.

External network connections

ICT Services are responsible for ensuring that all connections to external networks and systems conform to the Code of Connection and supporting guidance found in the Data Security & Protection Toolkit e.g. HSCN and partner NHS organisations.

Fault logging

ICT Services are responsible for ensuring that a log of all faults on the network is maintained and reviewed.

System change control

ICT Services are responsible for ensuring that appropriate change management processes are in place to review changes to ICT infrastructure and that changes that impact users are communicated in advance.

Configuration backup

ICT Services are responsible for ensuring backup copies of switch data stored on file and application servers, together with backups of ICT infrastructure e.g.network hardware configurations.

A log should be maintained of server backups detailing the date of backup and whether the backup was successful.

Documented procedures for the backup process will be produced and communicated to all relevant staff.

Physical security and environmental management of Core ICT equipment
ICT Services are responsible for the physical security and environmental management of core ICT equipment, including:

- Servers hardware
- Core network hardware
- Core IP telephony hardware
- Backup tapes
- Backup power supply for core hardware ie Uninterruptable Power Supply (UPS)
- Environmental monitoring systems

Access control to secure network areas

Entry to secure areas housing critical or sensitive network equipment will be restricted to members of the ICT services infrastructure team.

Monitoring tools
The status of all core ICT infrastructure will be monitored 24x7 by appropriate ICT management systems, which will alert ICT Services should there be a failure, so that corrective actions can be taken.

All laptop devices will be fully encrypted.

ICT core Infrastructure passwords
Passwords for core ICT infrastructure, sometimes called “system passwords”, will be changed every 6 months.
These passwords need to be a minimum of 10 characters in the length and should be complex, including numbers and letters.

20. Business Continuity

The trust has documented Business Continuity Business Continuity Plans (BCPs) for each service and department across the trust. This includes continuity plans for:

- Loss of staff
- Loss of building /workspace
- Loss of ICT, telephony and critical data
- Loss of equipment and/ or supplies

Guidance and advice is available on the emergency planning section of the intranet.

Business continuity arrangements are monitored through the Emergency Planning Sub Committee (EPSC) which is accountable to the Operational Committee. The EPSC is responsible for coordinating and developing business continuity planning across the organisation and identifying strategies to minimise potential risks to the functioning of the organisation. The EPSC is also responsible for reviewing, testing and developing the trust’s major incident plan and supporting strategies. The Chair of the EPSC escalates any issues that require executive action.

Appendix 1 - Unacceptable Behaviour

Examples of Unacceptable behaviour

The following list is indicative of behaviour which is not acceptable in respect of the use of CWP ICT infrastructure:

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using another member of staffs' username/password to logon onto any system
- Breaking into the system or unauthorised use of a password/mailboxSending or forwarding e-mails which contain Person Identifiable Information (PID) to non NHS email addresses unless it has been encrypted via the CWP email encryption service. NOTE: NHS email addresses either take the form of "@trustname.nhs.uk or "@NHS.net".
- Forwarding confidential email to external locations.
- Using e-mail to send offensive or harassing material to other users
- Using e-mail to send SPAM
- Transmitting unsolicited commercial, sales or advertising material
- Use of trust communications systems to set up personal businesses
- Distributing, disseminating or storing images, text or materials that might be considered offensive or abusive, in that the context is a personal attack, sexist or racist
- Accessing copyrighted information in a way that violates the copyright
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- Undertaking deliberate activities that waste staff effort or networked resources
- Deliberately introducing any form of computer virus into the corporate network
- Visiting Internet sites that contain obscene, hateful or pornographic Material
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Deliberately Accessing unauthorised areas of the Technical Infrastructure, including data, servers and communication devices.
- Circumventing user authentication or security of any host, network or account.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's logon session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Cheshire and Wirral Partnership NHS trust employees to parties outside Cheshire and Wirral Partnership NHS trust.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Deliberately effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, "hacking" such as 'network sniffing', 'pinged floods', 'packet spoofing', 'denial of service', and 'forged routing information' for malicious purposes.
- Postings by employees from a Cheshire and Wirral Partnership NHS trust email address to forums are not recommended unless posting is in the course of business duties.