Cheshire and Wirral Partnership NHS
NHS Foundation Trust

Document level: Trustwide (TW)
Code: IM1
Issue number: 3

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

Lead executive	Director of Operations
Author and contact number	Head of ICT Services - 01244 852 348

Type of document	Policy
Target audience	All CWP staff
Document purpose	To advise on the use of CWP's Information Communications Technology (ICT) services.

Approving meeting	Records and Clinical Systems Group	13/06/2016
Original issue date	Oct-06	
Implementation date	Mar-14	
Review date	Mar-19	

CWP documents to be read in conjunction with	HR6	Mandatory Employee Learning (MEL) policy
	GR3	Risk management policy
	IM7	Code of confidentiality policy
	GR12	Media policy
	IM6	Information sharing policy
	GR17	Freedom of Information (FOI) policy
	IM10	Information governance (IG) 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

Changes made with rationale and impact on practice
1. Full document review

External references

References
1. Misuse of Computers Act (1990)

To view the documents Equality Impact Assessment (EIA) and to see who the document was consulted with during the review click here.

Content

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 CWP to risks including loss of access to clinical systems like CareNotes and potential legal proceedings.

1.1 Scope

This policy applies to employees, contractors, consultants, temporaries and other workers at CWP, including all personnel affiliated with third parties. This policy applies to all staff who use equipment which is owned or leased by CWP.

1.2 User Identity

To access the CWP network, each member of staff is assigned a user account, together with an initial password which users are forced to change at first log in.

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 application such as CareNotes.

All network and application access is logged against each user account. It is therefore the responsibility of each user to ensure they don't share or divulge their password to anyone.

When logging on to the CWP networks (which are called CWPDOM / WCPCT), each user is agreeing to abide by this policy.

1.3 Agreement

All CWP employees, contractors or temporary staff who have been granted the right to use CWP's ICT infrastructure by their department manager, are required to acknowledge this agreement by confirming their understanding and acceptance of this policy. All staff agree to follow Trust policies when signing their contract of employment and the Records & Clinical Systems Group monitor breaches of this policy.

1.4 Breaches of this policy

All breaches should be logged with the CWP incident management system (Datix) and consideration should be made as to whether HR should be contacted to discuss possible disciplinary. Failure to comply with this policy can result in sanctions ranging from disciplinary procedures as per the disciplinary policy and procedures such as verbal and written warnings, through to dismissal.

In order to ensure compliance all CWP staff should be aware that email and internet usage is monitored to ensure compliance with legislation and policy by the ICT Services, failure to comply with duties which may result in dismissal or bringing criminal charges, disciplinary sanctions are as per the disciplinary policy and procedures.

No action should be taken by users or manages 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 servicedesk and appropriate action will be taken by ICT Services to secure the relevant ICT equipment.

2. ICT Network acceptable usage

2.1 Overview

The ICT network is a collection of communication equipment such as servers, PC's, printers, routers and switches, which has been connected together. The network is created to access applications like are clinical systems, CareNotes, MS Outlook, CWP Intranet and to share data (file shares) and peripherals, such as printers.

To ensure the integrity of the ICT network it is the responsibility of every computer user to be aware of this policy and to conduct their activities accordingly.

2.2 Access control to ICT network equipment and passwords

Only PC's, laptops and tablet devices that are owned by CWP and managed by ICT Services can be connected to the network.

Access to the network will be via an individual user account and associated password.

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 Servicedesk.

Users are responsible for ensuring their **password is kept secure**.

The password is required to be:

- A minimum of 8 characters in length;
- A combination of letters and numbers;
- Be changed every 35 days;
- And is not to be reused within 12 months of being used for the first time.

Should a user forget their password, they should contact the ICT Servicedesk to have it reset.

User access rights will be immediately removed or reviewed for those users who have left the trust or changed jobs.

Clinicial areas requiring shared tablet devices to access electronic patient records such as Carenotes for example in a ward setting, would normally be required to set an eight character strong passcode per individual staff user. The Mobile Device Management platform dictates that in order to enable tablet sharing a new strong passcode is set at every session. This has proved operationally challenging for staff to manage and has been deemed unfit for purpose. Therefore shared tablet devices will be set up with a shared passcode adhering to strong criteria but will be used by all staff. Whilst confidential information will be accessed on shared devices individual log ons will be required to access systems once the device is unlocked such as Carenotes, CWP email, and CWP intranet. As a further mitigation general internet access will not available as it is not fully auditable. Where multiple shared devices are used within the same team it will be necessary for the team to accept responsibility for coordinating passcode resets.

Some non-clinical areas use smartphones to access service specific mobile applications for example Estates staff using MiCAD and Zeta Mobile for work scheduling and Legionnella testing. The information contained within these applications does not relate to patients and is not senstive in nature.The standard passcode policy requiring an eight character strong passcode is restrictive whilst undertaking manual tasks and will be reduced to four digit numeric passcode to allow staff to operate these applications more effectively. Any devices configured with a four digit pin will not have access to CWPhosted systems.

2.3 General use and ownership

- Users are required to "lock" unattended PCs, laptops and tablets, if they are away from the desk. On Windows devices, this is achieved by pressing the CTRL-ALT-DEL keys at the same time;
- PC's, laptops and tablets will automatically be locked after 10 minutes of non use;
- ICT Services will display corporate desktop backgrounds and screensavers (and prevent them from being changed) on all computers logging on to the CWP network domain;

- 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;
- Because information contained on portable computers is especially vulnerable, special care should be exercised. See section 5 for use of laptops and other portable equipment.

2.4 Security and proprietary information

Information contained on all CWP 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: trust private, 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 Person 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.

2.5 Storage of user files

User files must be stored on an appropriate networked fileserver via the use of "networked drives" or "file shares" e.g. the "S:\" drive and must not be stored on a local hard disk drive or "C:" drive of a PC. This is to avoid any kind of data loss as:

- PCs are not backed up, whereby fileservers are backed up on a daily basis;
- Fileservers are usually kept in secure areas, unlike PCs, which are often in use in open non secure areas.

Staff who use laptops or tablets, may store files on the local hard disk drive, but it is **their reasonability to ensure that those files are periodically copied to a networked fileserver.**

NOTE: laptops and tablets have encrypted hard disk drives, thus minimising risks of data loss should the device be lost or stolen.

2.6 Ensuring computers are kept secure with Operating System and Anti-Virus updates

It is a mandatory requirement that all CWP PCs, 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 ultimately mean that systems are not accessible, like CareNotes and / or that "hackers" could access CWP systems.

Users of laptops and tablet devices must connect their device regularly to the CWP 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.

Should a virus alert be displayed on the screen of PC, laptop and tablet device, the users should disconnect the device from the network and call the ICT Servicedesk.

2.7 Unauthorised applications / software

- Only CWP approved applications / software can be installed on CWP owned PCs, laptops and tablet devices;
- Under no circumstances should staff attempt to install software;
- Users who are unsure if an application / software is approved for use by CWP can be directed to contact ICT Servicedesk for clarification;

- Any user, who discovers unauthorised software that has been installed on a CWP device, should contact the ICT Servicedesk to report it and have it removed.

2.8 Procurement of non-standard ICT hardware and software

Users wishing to purchase non-standard hardware or software are required to contact ICT Services to discuss their requirements. A review of requirements will be undertaken and appropriate hardware / software will be identified.

3. E-mail acceptable usage

3.1 Staff responsibility

The Trust makes use of 2 electronic mail services:

- An in house CWP system (Microsoft Exchange), with an email address format of firstname.surname@cwp.nhs.uk. This is used by most staff in CWP;
- The national NHS system, called NHS Email, with an email address format of name@nhs.net, which is used by CWP west physical health services staff.

3.2 The need for an electronic mail policy

The use of electronic communication has increased considerably within CWP and will continue to do so. As this demand increases so does the need to understand how this technology exposes CWP to legal liability.

The ease of email (quick, effective, cheap) encourages employees to adopt a more relaxed manner. It is seen as more akin to a verbal form of communication (telephone) rather than a formal, typed letter. However, the main difference between these two types of communication is that a telephone conversation is not formally recorded, whereas a written record is retained with an email. Thus, it is important to realise that emails can produce an evidential record.

In addition, unlike verbal communication, it is difficult to ascertain the tone of an electronic message and therefore bullying and intimidating reprimands through this medium, may lead to stress or personal injury claims by employees.

Electronic mail provides the ability to send messages, immediately anywhere in the world and to many people, simultaneously.

3.2.1 Electronic mail protocol

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

3.2.2 Personal email

During normal working hours an employee may only use the electronic mail service for business and clinical purposes only. However, to keep within the spirit of this policy, CWP will allow users to send and receive personal messages, during their own time, e.g. lunch breaks, and subject to gaining access to equipment if it is not needed by others in the course of their working duties. It is expected that personal email will be occasional and limited to text based messages.

These personal messages must have subject section of the email as “PERSONAL”, and by default, messages marked in this way are in no way whatsoever associated with CWP. The email professional conduct detailed below is also mandatory for personal emails and the storage of these must be limited to a maximum of two weeks.

3.2.3 Privacy

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

3.2.4 Confidentiality

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

These are transmitted over the secure NHS N3 Wide Area Network (WAN).

Emails containing PID that are required to be sent to non NHS third parties, are required to be sent via the CWP email encryption service, details of which can found on the CWP intranet at http://nww.cwp.nhs.uk/informatics/Pages/emailencryption.aspx

3.2.5 Email professional conduct

CWP expects the users of the electronic mail service to conduct their activities in a professional manner.

This policy makes it clear that electronic communication, used for business and clinical purposes, **must** be treated the same way as formal business correspondence. Therefore, when addressing other email users within CWP, each message should contain the sender's name, job title and department.

When communicating externally, the sender's address must also be included as part of the message. 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.

3.2.6 Email content

Users are prohibited from sending emails that may be deemed as:

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

The email systems should only be used for business relating to CWP, except for the occasional personal use, as detailed above.

Users should not use it for any commercial or illegal activities i.e. selling items that require a license – tobacco / alcohol.

3.2.7 Computer viruses

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

3.2.8 Deletion of emails

Users are advised that the "deletion" of an electronic mail message, does not guarantee that the message has been permanently erased. Thus for the purposes of this policy, users need to be aware that a permanent record of their deleted messages may exist until such time that the email system backup tape has been overwritten.

3.2.9 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 email users must ensure that the relevant facts are set out.

3.2.10 Compliance with trust standing financial instructions

As organisations embrace electronic communications the ability to order goods and services electronically is becoming simplified. These organisations may also accept electronic messages as orders for goods and services. Compliance with CWP Standing Financial Instructions (SFI) is mandatory at all times.

3.2.11 Use of non NHS web based email services

Guidance on the use of web based email services, such as Gmail, MSN, or Yahoo etc, is detailed in the "internet acceptable usage" section in this policy.

4. Internet acceptable usage

4.1 Purpose

The purpose is to clearly define the permissible use of the internet by authorised staff in the CWP.

This also includes staff who are not employed by CWP but who have authorised access to the Internet through the computers owned or managed by CWP.

To ensure compliance with this policy all internet access is logged by individual user account and retained for audit purposes.

Failure to comply with this policy may result in disciplinary action being taken as per the disciplinary policy and procedures, which may result in dismissal or criminal prosecution.

4.2 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 website as they are deemed inappropriate for viewing within the workplace or have limited bandwidth assigned to them to deter abuse e.g. YouTube.Com.

4.3 Responsibilities of the user

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

4.3.1 Permissible access

All staff have access to the internet via computers located throughout the various CWP 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 CWP internet service for reasonable, personal use on their own time, e.g. during lunch breaks, 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. Line managers may request monitoring of personal usage of staff.

4.3.2 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, e.g. serious breach of confidentiality, CWP is the final arbiter that is that CWP will have the final decision on what is or is not offensive material, or what is or is not permissible access to the internet.

4.3.3 Unsolicited emails

Users should be aware of certain types of unsolicited email, sometimes known "fishing / phishing emails", that pretend to be from trusted sender, e.g. "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 Servicedesk to alert them of the incident.

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.

4.3.4 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 logged as an incident on Datix as per the incident reporting and monitoring policy.

4.3.5 Downloading files

CWP 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 Servicedesk must be followed.

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

4.3.6 Social Media

CWP 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 CWP 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.

4.3.7 Use of non NHS web mail services

Users can make use of non NHS Web mail services, like Gmail, MSN or Yahoo etc, but this is to be done in their own time and with the permission of their line manager. Attachments to such emails, must not be opened or download, as they may contain a virus.

4.3.8 Confidentiality

You are bound by the code of confidentiality policy and security policy of CWP 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 CWP outside the organisation.

5. Usage of laptops, tablets and smart phones

5.1 Objectives

CWP recognises and accepts its responsibilities associated with the safe use of laptops, portable ICT equipment and removable computer media. CWP, in approving this policy, sets the standards to be achieved within the organisation and expects the co-operation and involvement of its managers and staff (see mobile devices policy).

5.2 Staff responsibility

CWP staff that use laptops, portable computer equipment and removable computer media must ensure they adhere to policy and its objectives, especially that their use of these devices and media is specifically for work related purposes only. Failure to comply with this may lead to disciplinary action as per the disciplinary policy and procedure. If a member of staff resigns from their post they must return all equipment and removable computer media to their line manager, before leaving.

5.3 The need for this policy

The use of laptops, portable ICT equipment and removable computer media has increased significantly within CWP and this increased usage exposes CWP to greater risks as these devices, along with the sensitive data stored within them, are taken outside of the secure CWP environment.

This type of equipment and media may be lost or stolen, or subject to unauthorised access or tampering, accidental or deliberate and it may also be confiscated by the relevant authorities such as the police as crime evidence. Loss of an individual device or media could affect CWP's reputation significantly. Furthermore if the data it contained was compromised and this led to the disclosure of patient or other sensitive information, the impact to CWP would be highly significant as patients and staff would lose confidence in the CWP's ability to protect their personal data.

5.4 Definitions of portable ICT equipment and removable computer media

Portable ICT equipment and removable computer media (subsequently referred to as *equipment and media*) can be classified as any type of device which can be used to store or move data. Examples are as follows:

- Laptops;
- Personal Data Assistants (PDA's);
- Smart phones;
- Blackberry's;
- Tablet and slate computers;
- Memory sticks;
- Floppy discs;
- Re-writeable CD and DVD's;
- Magnetic tapes;
- Portable hard drives;
- Secure digital cards.

Where practical, equipment and media should be permanently marked, to identify that it belongs to the CWP and this marking must not be removed or altered in any way.

5.5 Authorisation of allocation of mobile devices

Any person taking equipment and media off-site must have signed authorisation from their line manager. This authorisation must include the identity of the equipment and media and the purpose for which it is to be used.

5.6 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 CWP incident reporting and management policy.

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

Equipment and media can be used to store these types of information for work related purposes only and it 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 8 characters

- Combinations of letters and number (don't use obvious combinations e.g. abcd / 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.

5.8 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 health records policy for classification descriptions.

5.9 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 servicedesk. 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.

5.10 Internet access via non CWP networks

CWP portable equipment can be used to remotely access CWP systems via internet or 3 party networks e.g. home broadband, public WiFi or partner organisations, but **MUST** be used in conjunction with a CWP remote access fob (CWP current standard is a Vasco device) to create a secure connection and in conformance with CWP's internet usage policy.

5.11 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 CWP, using an approved security cable;
- At the end of working hours, laptops and tablets, should be placed in secure local location e.g. desk draw;
- When offsite 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 and not left overnight in cars;
- 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.

6. Third parties bringing ICT equipment and removable media into the organisation and connecting to the CWP Network

6.1 ICT Equipment

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

6.2 Media

Any third party wishing to use removable computer media within CWP for work related purposes, such as presentations, is only authorised to use this media in non-networked CWP 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.

7. 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 Servicedesk, 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:

- For floppy discs, CD ROMs, and DVD's please contact the local estates department who can arrange shredding on your behalf;
- For all other media please contact the ICT Servicedesk for advice.

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 reusing removable computer media please contact the Servicedesk for further information

7.1 Incident reporting

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

- Your line manager or their deputy;
- ICT Servicedesk - so that any containment action can be taken accordingly;
- Logged as incident on the CWP incident management system (Datix);
- The CWP lead for clinical governance;
- In the event of equipment loss / theft, this should also be reported to the relevant Police Service. See fraud, theft and corruption policy.

8. Responsibilities of ICT Services

8.1 NHS statement of compliance

The staff within the ICT Services are acting as the delegated agents of the Chief Executive are responsible for maintaining a safe and secure computing environment in CWP.

More specifically they are responsible for ensuring that CWP conforms to Information Governance and Statement of Compliance regulations.

8.2 Monitoring and blocking internet access

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

Should a line 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. Currently, this will cover up to 3 months internet access history.

If a member of staff has been accessing or trying to access an inappropriate website, it is the responsibility of the ICT Services staff to notify the Servicedesk manager or deputy, who in turn will contact users line manager and ask them take appropriate disciplinary action. Please see disciplinary policy and procedure.

If line manager requires the member of staff's user account to be suspended, they should make that request to Servicedesk manager, via email and if it is time critical, follow up with a phone call to Servicedesk manager, via the Servicedesk.

8.3 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 CWP;

- Undertaking regular audits to support these functions.

8.4 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.

8.5 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.

8.6 Maintenance contracts

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

8.7 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 Information Governance Toolkit (IGT) e.g. N3.

8.8 Fault logging

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

8.9 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.

8.10 Configuration backup

- ICT Services are responsible for ensuring that 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.

8.11 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 i.e. Uninterruptable Power Supply (UPS);
- Environmental monitoring systems.

8.12 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.

8.13 Monitoring tools

The status of all core ICT infrastructures 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.

8.14 Third party access to the network

Third party access to the network will be based on a formal support contracts that satisfies all necessary NHS security conditions.

8.15 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 8 characters in the length and should be complex, including numbers and letters.

9. Business Continuity

CWP has documented Business Continuity Plans (BCP) for each service and department across CWP. This includes continuity plans for:

- Fire, flood, impact damage;
- Equipment and component failure, severe capacity restriction;
- Power supply withdrawal;
- Malicious attack including physical and network / system intrusion;
- Theft of information and media (including paper) resulting in unavailability of information.

BCPs are accessible on the emergency planning section of the intranet.
Business continuity arrangements are monitored through the Emergency Planning Sub Committee (EPSC). The EPSC is accountable to the Operational Board and is responsible for co-ordinating 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 CWP's major incident plan and supporting strategies. The chair of the EPSC escalates any issues that require executive action.

Appendix 1 - Examples of unacceptable behaviour

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

- Using another member of staffs username / password to logon onto any system;
- Sending or forwarding emails 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 email to send offensive or harassing material to other users;
- Using email to send SPAM;
- Use of CWP 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;
- Breaking into the system or unauthorised use of a password / mailbox;
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters;
- Transmitting unsolicited commercial, sales or advertising material;
- 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, CWP employees to parties outside of CWP;
- 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;
- 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;
- Postings by employees from a CWP email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CWP, unless posting is in the course of business duties.