Information Communication Technology Policy

Department / Service:	Digital Division
Accountable Director:	Vikki Lewis – Chief Digital Officer
Approved by:	Information Steering Group
Date of approval:	12th June 2023
Next Revision Due: This is the most current document and is to be used until a revised version is in place	12th June 2026
Target Departments	All
Target staff categories	All

Policy Overview:

The aim of this policy is to ensure a consistent approach and delivery of ICT services exists for all staff. This approach is to set out and document the implementation, maintenance and management of ICT support services, clinical applications, and access to other ICT services by 3rd parties. This policy supports other Information Governance policies to provide a complete framework for safe and effective use of ICT services and the management of information.

This policy applies to:

- Worcestershire Acute NHS Trust Staff and 3rd Parties that use or have use of the ICT infrastructure located in WAHT sites.

The purpose of the policy is to provide a balance between security, ease of use for Digital services and to take full account of NHS guidance and legislation.

Latest Amendments to this policy:

Brief overview of amendments made to this policy when reviewed.

Added Digital Privileged Access Management Policy .6.3
Added Third party/supplier access policy/procedure 6.4
Added updates to Password policy to include recommendations from DSPT toolkit

Contents:

Page

Appendices

Supporting Documents

2. Policy Context

The Information Communication & Technology Policy (ICTP) has been developed to provide governance for the appropriate access and use of electronic systems; clinical and non-clinical, endpoint devices and other ICT related assets. The policy enables information to be shared, but ensures the secure protection of that information and related ICT assets. The policy will protect the Trust and its employees from ICT hazards and threats, to ensure business continuity and to minimise any business damage by preventing and reducing the impact of infrastructure and information systems incidents.

2.1 Policy Requirement

- To ensure the effective operation of ICT infrastructure, information systems and that those systems are delivered when and where they are needed, by maintaining their confidentiality, integrity and availability.
- Ensuring that all Trust staff and any Trust appointed contractors are aware of and comply with the relevant legislation as described in this and other associated policies.
- Describing the principles of security and explaining how they shall be implemented in the Trust.
- To introduce a consistent approach to information security within the Trust, ensuring that all members of staff understand their own responsibilities.
- Creating and maintaining, within the Trust, a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information that is stored within, on or by assets under the control of the Trust.
- Provide appropriate governance of ICT related assets for their use, sharing of information and management of risk related to use and access.

This policy applies to all electronic information media, such as Trust supplied USB encrypted memory sticks, computers, mobile devices, cameras, Dictaphones, information systems such as Evolve, Bluespier, ICE, Winpath, Patient First and PACS. Trust computer networks, applications, locations in use by Worcestershire Acute Hospitals Trust (WAHT) or their staff and organisations hosted by WAHT or supplied under contract to it.

2.2 Rationale (Why)

This document defines the Information Communication & Technology Policy (ICTP) for Worcestershire Acute NHS Hospitals Trust, hereafter known as WAHT. It forms a key component of WAHT overall information governance management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.
The ICTP applies to all Trust business and covers the information, information systems, networks, and physical environments where information is processed or stored.

The objectives of this ICTP are to ensure the effective operation of information systems and that those systems are delivered when and where they are needed. It will preserve:

- **Confidentiality**
  Access to data or information is confined to those who have legitimate authority to view it.

- **Integrity**
  Data or information shall be complete, timely, accurate and detected or amended only by those specifically authorised to do so. All systems, assets and networks shall operate correctly, according to specification.
- **Availability**
  Information shall be available and delivered to the right person, at the time when it is needed.

Users must be aware of their responsibilities as detailed in this policy, so these objectives aren’t compromised.

2.3 Principles

The aim of this policy is to ensure users have a framework to govern the access to ICT and associated services. Also to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WAHT by:

- Providing a safe, secure and stable ICT infrastructure
- Providing guidance on access to information using ICT equipment
- Providing information on how to access support services
- Ensuring that all members of staff are aware of and comply with the relevant legislation as described in this and other associated policies.
- Describing the principles of security and explaining how they shall be implemented in the Trust.
- Introducing a consistent approach to security, ensuring that all members of staff understand their own responsibilities.
- Creating and maintaining within the Trust, a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the Trust.

2.4 Scope

This policy applies to all staff in relation to the use of applications, electronic information, storage of information, including Data Loss Prevention (DLP), Encryption, and the associated media, such as Trust supplied USB encrypted memory sticks, computers, mobile devices, cameras, Dictaphones. Including, but not limited to, information systems such as Oasis, Evolve, Bluespier, ICE, Winpath, Patient First and PACS. Trust computer networks, applications, locations in use by WAHT or their staff and organisations hosted by WAHT or supplied under contract to it.

3. Responsibilities and Duties

3.1 Chief Executive Officer

Information security is the responsibility of all staff within the WAHT. Ultimate responsibility for information security resides with the Chief Executive. This responsibility should be discharged through a designated senior member of staff who has lead responsibility.

3.2 Chief Digital Officer

The Chief Digital Officer has delegated executive accountability for all Digital services within the Trust, including Information Communication and Technology and Information Security, on behalf of the Chief Executive Officer. The day to day activities required to effectively implement and maintain this policy with be performed through the Chief Technology Officer.

3.3 Senior Information Risk Owner (SIRO) – Chief Finance Officer

The Trust's SIRO is accountable for fostering an information security aware and focused culture that protects data, providing a focal point for managing information risks and incidents and is concerned with the management of all information assets.

3.4 Senior Information Asset Owner (SIAO) and Information Asset Owner (IAO)

An IAO's role is to understand and address risks to the information assets they 'own'; provide assurance to the SIRO on the security and use of these assets. SIAO, will have at least one Information Asset Owner (IAO) will be designated for each information system within the Trust prior to that system being implemented for use within the Trust. The IAO will ensure that the Information Security Policy and associated procedures are enforced within their areas of responsibility.

The Senior Information Asset Owner is responsible for providing the assurance that a business impact assessment, business continuity and disaster recovery plan exists and is fit for purpose. Also to provide assurance that annual risk assessments for their application are maintained and managed accordingly.

The Digital Division with the assistance of Computacenter, will provide risk assessments, a business continuity plan and disaster recovery plan for the ICT infrastructure.

3.5 Information Asset Administrator (IAA)

An IAA will provide support to IAOs by: ensuring that policies and procedures are followed, recognising potential or actual security incidents, consulting their IAO on incident management and ensuring that information asset registers are accurate and maintained up to date. The Information Asset Administrator (IAA) will be responsible for the day-to-day management of that system; including a system specific Information Security Policy, Information Asset Registration and Risk Assessment.

3.6 Caldicott Guardian

The Trust's Caldicott Guardian (Chief Medical Officer) has a strategic role in ensuring that there is an integrated approach to information governance, developing security and confidentiality policy and representing confidentiality requirements and issues at Board level.

3.7 Chief Technology Officer (CTO)

The Chief Technology Officer has overall responsibility for the maintenance, implementation and enforcement of the ICT Policy. The CTO will provide assurance to the CDO and SIRO that the management and security of the Trust information, technology and communications systems and infrastructure are able to meet national compliance, regulatory and statutory requirements.

3.7.1 Digital Security Manager (DSM)

The Digital Security Manager is responsible for the day to day management of information security practices and procedures. Their responsibilities include:

- Ensuring that information technology policies, information security procedures and working practices align themselves to the ICT Policy.
- Monitoring and reporting on the status of ICT security within the Trust.
- Ensuring compliance with relevant legislation and regulation.
- Working with the Emergency Planning, Resilience and Response (EPRR) Manager, Computacenter, Information Governance and Trust managers to ensure all staff and contractors are aware of their responsibilities and accountability for information security
- Working with Computacenter to ensure that active monitoring for potential security breaches occurs and providing reports or briefings to the relevant governance forums in relation to outcomes and findings from monitoring.
- Working closely with those responsible for Freedom of Information, Data Protection, patient confidentiality and other Information Governance work areas.
- Providing direct input to the information security components of the IG Toolkit.

3.8 Information Governance Manager

In addition to the Information Security Manager, the Trust has an Information Governance Manager responsible for:

- Information Governance Management
- Confidentiality and Data Protection
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance.
- Work with Information Asset Owners (IAO) to ensure that assessments are completed to discover any non-conformities and associated improvement/treatment plans are drafted and implemented to accept, reduce or eliminate the risk of the non-conformity

In addition there exists a Worcestershire Countywide Information Governance Steering Group which comprises the Information Governance Managers from each Worcestershire Health and Social Care Organisation, the SIRO (Or their nominated Deputy), the Information Security Managers (or staff member with that role in their Job Description) for each Trust and the Computacenter Account Information Security Manager. Through this group, common approaches are agreed to aspects of Information Governance where appropriate. Together they have responsibility for completion of the IG Toolkit for their own organisations.

3.9 Computacenter

Computacenter provide IT support services and are contractually responsible for the maintenance, support and administration of the Trust’s infrastructure service. They are managed via contract to ensure the day to day IT infrastructure services required to enable patient care are available and comply with any security requirements that the Trust must achieve or meet, such as the NHS Data Security and Protection Toolkit (DSPT). They are contractually obliged to provide assurance that the services they proved are robust and resilient. These contractual obligations/service provisions include, but are not limited to:

- Supplying a staff member with a network login, an Email account, system and Internet access. Computacenter must ensure that there are systems and procedures in place to prevent or identify breaches of security and means of taking action against the offending parties.

Computacenter will:

- Ensure that the starters, leavers and changes process is followed for short term, fixed term and permanent staff is followed to provide access to the Trust network and end point devices.
- Use filtering and content management tools to monitor Internet usage and inbound/outbound emails to ensure security of the WHITS network system.
- Using management and monitoring tools actively manage the capacity, availability, security and integrity of the ICT infrastructure (Wi-Fi, structured cabling, servers, network switches and end point devices), access to these infrastructure assets and report on non-conformities to the Digital Security Manager
- Manage and maintain the Trust's ICT infrastructure in accordance with this policy and the agreed contract(s) between the Trust and Computacenter.
- Ensure that any inappropriate use of the internet will be identified and reported to the appropriate line manager, IG Lead Manager, Caldicott Guardian and/or Human Resources.
- Implement, manage and maintain Trust anti-virus software on servers, PCs and laptops.
- Anti-Virus on mobile devices will be implemented, managed and maintained by the Unified Communications and Collaboration Manager
- Ensure that access to certain websites may be restricted based on Trust requirements
- Implement security measures, as directed by the Trust, to protect the information stored in the Trust infrastructure from unauthorised access.
- Provide reports and base data relating to all incidents and requests made by staff relating to ICT security and infrastructure.
- Work with the Trust to provide information security responses and advice in line with the Trusts ICT and IG obligations
- Responsible for ensuring that any Computacenter staff used on site are aware, understand and abide by this policy and all other Trust polices while working for Worcestershire Acute Hospitals NHS Trust.

3.10 Directors and Departmental Managers

Directors and departmental managers must ensure:

- They keep appraised of all information security and governance guidance issue by the Trust
- That all staff they have responsibility for are appraised of all information security and governance guidance issue by the Trust
- That staff have appropriate secure access to systems and have up to date training for the systems they are using
- That staff know how to access the advice on information security matters using the intranet
- That appropriate levels of access are granted to specific individuals (e.g. Registration Authority role for staff who issue smartcards) to perform their role
- Ensure that all staff sign confidentiality agreements as part of their contract of employment
- Ensure that Digital, RA and system managers are informed of staff role changes, new starters and leavers.
- The security of physical environments where information is processed or stored within their area
- When systems from third parties are to be implemented, underpinning contracts will be introduced to ensure that the staff or sub-contractors of the third party shall comply with all appropriate security policies and procedures.
- Applications are not introduced into the Digital environment, without appropriate approval from the Digital Division.

3.11 Individual staff

All staff, including contract and temporary workers are:

- Responsible for conformance to the ICT Policy, associated policies, guidelines and best practice.
- Expected to report information security incidents by logging the incident on the Trust Datix system and the NGSD system, ensuring that the Datix reference is captured in the log.
- Ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard
- Required to sign a general statement of confidentiality on commencement of employment.
- Required to sign the User Responsibility Statement that is contained within the Information Security Declaration (Appendix 1 of this document). This is as an indication that they accept responsibility for maintaining security and confidentiality and that they understand the consequences of any breach.

3.12 Contractors and 3rd Parties

Contractors and 3rd Parties must abide to the requirements set out in this policy and in addition to the responsibilities for individual staff, as detailed above, a contractor must:

Ensure that any device connecting to the Trust infrastructure or systems are:

  - Up to date on with the Operating System security patches
  - Have up to date and active antivirus installed
  - Ensure any Trust information that is required to be transferred is encrypted.

Any requirement to store the Trust's data on an end point device must be specifically authorised by the responsible Trust manager and where appropriate, if Person Identifiable Information (PII), Commercially Sensitive Data or other Trust sensitive information is involved, the Caldicott Guardian/Information Governance Manager/Information Asset Owner (IAO)/Senior Information Risk Owner (SIRO).

The end point device must be encrypted to the required level, as detailed in this policy; this can be verified with Computacenter as specified by Worcestershire Acute Hospitals NHS Trust.

The ICTP will be maintained, reviewed and updated by the Digital Security Manager in conjunction with Chief Technology Officer. The Computacenter Security Manager and SIRO (or their nominated deputy) shall review draft policies prior to approval in accordance with Trust guidelines relating to policy review, unless a significant change is required.

3.13 Management of Security

- At Trust Board level, responsibility for information security resides with the SIRO.
- The Chief Technology Officer, with support from the Digital Security Manager, is responsible for implementing, monitoring, documenting and communicating information security requirements for the Trust.
- The Information Technology and Security Forum (ITSF) will discuss, monitor, manage and recommend information security measures in the first instance and then provide the recommendations to be ratified by the Information Governance Steering Group (IGSG).
- The Chief Technology Officer, or by delegation the Digital Security Manager, will provide assurance to IGSG, Digital SMT and Audit and Assurance Committee for all information security.

3.14 Information Security Awareness Training

- Information security awareness training must be provided to all staff while employed by the Trust or working for a 3rd party on behalf of the Trust. This includes receiving training at induction, receiving regular Intranet updates and at team briefings.
- An on-going awareness programme must be maintained in order to ensure that staff awareness is refreshed and updated as necessary. This will be delivered to Trust staff in a number of mediums, including but not limited to -
  - Intranet notices and blogs,
  - Team meetings,

- Staff briefings,
- Trustwide emails,
- Statutory and Mandatory training,
- Policy and procedural updates.

3.15 Contracts of Employment

- Trust security responsibilities for staff should be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause.
- Information security expectations of staff are included within appropriate job descriptions.
- The ICTP must be sent to all new starters as part of the unconditional offer process. This will enable new starters to read, sign and return the User Responsibility Statement (see appendix 1), which will speed up the new starter process. Signed copies of the User Responsibility Statement must be kept within a staff members personnel file
- All staff, short term, fixed term and permanent staff, will sign the confirmation statement. However, where this is not practically possible for short term staff, the relevant policies should be provided to recruiting agencies for their staff who will be employees of the Trust. This provides assurance to the Trust that these resources know, understand and will adhere to the Trust policies while they are in the Trust's employment.

4. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis, by the appropriate IAO. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage these risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements must be a regularly reviewed feature of the ITSF. These reviews shall help identify areas of continuing best practice and possible weaknesses, as well as potential risks that may have arisen since the last review was completed. During these reviews, if a risk is categorised in the red section of the risk matrix, these risks should be highlighted to the risk department for inclusion on the Trust risk register.

5. Digital Support Services

The ICT team and Computacenter work together to ensure that ICT systems are supported, managed and maintained in a structured and efficient manner. The ICT team follow the ITIL framework to support and manage the ICT infrastructure.

Computacenter provide a number of ICT support services on behalf of the Trust:

- Service Desk, Incident Management and Problem Management

- Desktop Systems
- Server System
- Data Network Systems
- RAS and Internet Access
- User Catalogue and Procurement
- Asset Lifecycle Management
- Technical Design and Architecture
- BAU Hardware Replacement
- Data Storage Management
- IT Security Support
- Availability and Service Continuity
- Testing and Acceptance of Infrastructure Services
- ICT Project Consultancy and Delivery

The Trust ICT staff provide the following services to the Trust:

- Clinical Application Support
- Business Analysis
- Software and Clinical Application Testing
- Software Development
- ICT Training
- Information Security
- Infrastructure Operational Management
- ICT Project Management

The contract between the Trust and Computacenter details all aspects of the services they provide and the contract is managed by the Digital Division, Procurement and Finance.

Computacenter provide these support services which are managed to a Service Level Agreement (SLA), which are detailed below.

Priority code	Title	Description	Resolution Target Times
1	Clinical or organisational critical	An Incident which involves a complete or partial loss of a clinical or organisational critical service or the loss of key functionality affecting multiple Users and/or the availability of one or more clinical or organisational critical applications (including data integrity) at one or more locations, resulting in a significant clinical or organisational impact that prevents one or more functional units from operating.	The Supplier must resolve Priority 1 Incidents within four (4.0) Service Hours
2	High	An Incident which involves a complete or partial loss of service or functionality affecting multiple users and / or the	The Supplier must resolve Priority 2

		availability of one or more supported applications (including data integrity) at one or more locations, resulting in a material clinical or organisational impact that prevents one or more functional units from operating effectively.	Incidents within eight (8.0) Service Hours.
3	Standard	An Incident that impacts directly upon one or more users; where an immediate work round is not available, but there is no material clinical or organisational impact. For example, User unable to access Microsoft Word; user unable to print	The Supplier must resolve Priority 3 Incidents within one (1.0) Working Day
4	Non-Urgent	An Incident that impacts directly upon one or more Users; where an immediate work round is available, but there is no material clinical or organisational impact.	The Supplier must resolve Priority 4 Incidents within two (2.0) Working Days.
		Service Requests	
Service Request	Standard	For Service Requests	The supplier must complete requests within five (5.0) Working Days.

The infrastructure support tiers are defined below and they define what resilience and backup scheduling/maintenance are in place to manage application availability and restoration.

- Platinum – These are business critical applications or infrastructure
- Gold – These are business essential applications or infrastructure
- Silver – These are business core applications or infrastructure
- Bronze – These are business supporting applications or infrastructure

5.1 Support Portal Access

All staff have been provided access to use the ICT support services for reporting an ICT incident or/and ICT request through the Next Generation Service Desk (NGSD) portal. All staff are issued with a unique username and password to access the portals. Access to the portal is through authentication by the network login of a staff member.

The ICT Servicedesk is open 24 hours a day, seven days a week, and 365 days of the year. All calls to and from the ICT ServiceDesk are recorded for quality and training purposes.

An ICT incident must be logged if ICT hardware or software is broken or not working as expected. Incidents can be logged via the NGSD portal - https://ngsd.worcsacute.nhs.uk, either through the incident logging process or by using the webchat function. Webchat is available 8am – 6pm Monday to Friday. By telephone – **0800 085 4949** using the Intelligent IVR function. Staff will need to know their Employee/Payroll Number to log an incident.

An ICT request must be logged when you would like something new (software or hardware) or gain access to a service you never had access to before. Requests must be logged via the NGSD Portal only - https://ngsd.worcsacute.nhs.uk

Every request that you raise will require approval by your line manager before any action can be taken. Some requests will require a secondary approver for it to progress.

The servicedesk is the first point of contact for all ICT incidents. The servicedesk team will triage the incident and manage the call appropriately to the relevant team for resolution.

ICT have a section on the Intranet that has our vision, the departmental structure, user guides, help documentation and further information to assist staff with the use of ICT - http://nww.worcsacute.nhs.uk/departments-a-to-z/acute-ict/

6. Access Controls

System and network access controls do not only relate to staff access of endpoint devices (PCs, laptops and other mobile devices), but also to physical and logical domains in the Trust that hold confidential information. Access to all types of information is controlled, dependant on a staff member’s role and requirement. All breaches (non-conformities) of access control must be reported to the ICT service desk in the first instance, which will be investigated as part of the incident log. If there are additional investigations relating to the breach, all recommendations must be passed to the ITSF. This forum will review the investigation(s) and recommendations and provide a unified set of recommendations to the Information Governance Steering Group (IGSG). Any recommendations or changes approved at IGSG will be implemented in line with Trust policy.

6.1 Physical Access to controlled ICT areas

The Trust datacentres are managed to best practice industry standard and are equivalent to Tier 3 standards and ISO 27001 for Information Security. Only authorised personnel who have a justified and approved business need will be given access to the Trust datacentres, hub rooms and other restricted areas containing information systems or electronic data storage hardware. Each area will be managed by ICT and have swipe card locking mechanisms. These areas are accessible to ICT support staff and the appropriate on site staff, where necessary. When access to a secure ICT area is required staff will request access via NGSD - https://ngsd.worcsacute.nhs.uk

Standard lead time for access is five days and 3rd party suppliers will be escorted by a Computacenter staff member, or system administrator. All access to secure ICT areas will be logged electronically and have an Access Control Sheet for signing in and out. Any non-conformity will be reported and investigated and the relevant action or remediation will be taken in line with Trust disciplinary, where necessary, and Information Governance policies.

6.2 Logical Access

All users/staff members will have role-based access to ICT equipment and information – Clinical or non-clinical. Trust staff must follow the defined starters, changes (movers) and leavers policies and processes to have access granted. These policies are covered in HR policies and ICT guidelines that are available on the Intranet. Where new starters are required for a short term period – less than 5 days (locum doctors, agency staff or contractors, there are established processes to enable quick, short term access to information and systems. All other staff members must follow the standard new starters, movers and leavers process that is in place.

Logical access to endpoint devices are controlled by Information Governance and ICT policies and implemented by Digital ICT. The User Responsibility Statement for access to Trust owned endpoints must be signed by the staff member before any access to information is given.

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.3 Digital Privileged Access Management Policy

Digital Privileged Access Management (DPAM) is a set of policies and procedures designed to manage privileged access to digital systems and data. DPAM includes the granting, reviewing, and revoking of access to users who require elevated access to perform their job functions. This policy outlines the procedures for managing privileged access requests, including time-bound elements, to ensure that access to digital systems is managed in a secure and controlled manner.

Policy Statement:

Our organisation recognises the importance of managing privileged access to digital systems and data. To this end, we have implemented a Digital Privileged Access Management policy that outlines the procedures for granting, reviewing, and revoking privileged access to users who require elevated access to perform their job functions. All access requests must be submitted through our IT service desk system (NGSD), and all requests must include time-bound elements.

Granting Access:

Access to digital systems and data that requires elevated privileges must be approved by the Digital department. All access requests must be submitted through our IT service desk system (NGSD) and include the following information:

- Name of the user requesting access
- Reason for the access request
- Systems or data to which access is requested
- Manager's approval
- Time frame for access (start and end date)

The Digital department will review the access request and approve or deny access based on the user's job function and the principle of least privilege. Access is granted only for the specific time frame requested in the access request.

Access Review:

All privileged access requests must be reviewed periodically to ensure that access is still necessary and appropriate. Access reviews are conducted at least every six months and include the following steps:

- Review of the user's job function to ensure that access is still necessary
- Review of access logs to ensure that access has not been abused
- Approval or denial of continued access based on the results of the review

Access Revocation:

Access to digital systems and data is revoked automatically at the end of the time frame specified in the access request unless a new access request is submitted and approved. Access can also be revoked at any time if it is determined that the user no longer requires access or if there is evidence of abuse.

Audit and Compliance:

All access requests, approvals, denials, and revocations are tracked and recorded in our IT service desk system. This information is reviewed and audited regularly to ensure that access controls are effective and comply with applicable laws and regulations.

Conclusion:

By implementing this Digital Privileged Access Management policy, we aim to ensure that access to digital systems and data is managed in a secure and controlled manner, minimizing the risk of unauthorized access and data breaches. This policy helps to protect the confidentiality, integrity, and availability of our organisation's digital assets and ensures that access is granted only to users who require it to perform their job functions.

6.4 Third party/supplier access policy/procedure

Digital third-party/supplier access policy/procedure is a set of policies and procedures designed to manage access to digital systems and data by third-party vendors or suppliers who require access to perform their contractual obligations. This policy outlines the procedures for managing third-party/supplier access requests, including time-bound elements, to ensure that access to digital systems is managed in a secure and controlled manner.

Policy Statement:

Our organisation recognizes the importance of managing third-party/supplier access to digital systems and data. To this end, we have implemented a Digital Third-Party/Supplier Access policy that outlines the procedures for granting, reviewing, and revoking access to third-party vendors or suppliers who require access to perform their contractual obligations.

All access requests must be submitted through our IT service desk system and include time-bound elements.

Granting Access:

Access to digital systems and data by third-party vendors or suppliers must be approved by the Digital department. All access requests must be submitted through our IT service desk system and include the following information:

- Name of the third-party vendor or supplier requesting access
- Reason for the access request
- Systems or data to which access is requested
- Contractual obligation for access
- Manager's approval
- Time frame for access (start and end date)

The Digital department will review the access request and approve or deny access based on the third-party vendor or supplier's contractual obligation and the principle of least privilege. Access is granted only for the specific time frame requested in the access request.

Access Review:

All third-party/supplier access requests must be reviewed periodically to ensure that access is still necessary and appropriate. Access reviews are conducted at least every six months and include the following steps:

- Review of the third-party vendor or supplier's contractual obligation to ensure that access is still necessary.
- Review of access logs to ensure that access has not been abused
- Approval or denial of continued access based on the results of the review

Access Revocation:

Access to digital systems and data is revoked automatically at the end of the time frame specified in the access request unless a new access request is submitted and approved. Access can also be revoked at any time if it is determined that the third-party vendor or supplier no longer requires access or if there is evidence of abuse.

Audit and Compliance:

All access requests, approvals, denials, and revocations are tracked and recorded in our IT service desk system. This information is reviewed and audited regularly to ensure that access controls are effective and comply with applicable laws and regulations.

Conclusion:

By implementing this Digital Third-Party/Supplier Access policy, we aim to ensure that access to digital systems and data by third-party vendors or suppliers is managed in a secure and controlled manner, minimizing the risk of unauthorized access and data breaches. This policy helps to protect the confidentiality, integrity, and availability of our organisation's digital assets and ensures that access is granted only to third-party vendors or suppliers who require it to perform their contractual obligations.

7. Usernames, Passwords and Password protection

7.1 Password Management

A username and computer password – Network Login (AKA WHITS Login) is the first line in maintaining a secure and safe information and digital environment. The combination of these elements enable staff to gain access to systems, that are relevant to your role, which the Trust provides and also confirms identity in an electronic format. **Staff must not share your username and password or provide other staff members access to systems, as these are unique, just like a phone number or fingerprint. If staff knowingly allow other staff members misuse provided access to systems, that staff member will also be held responsible for the breach and disciplined accordingly.**

Trust staff are required to have a computer password (Active Directory) that must be a minimum of 15 (fifteen) characters long and should use the 3 or 4 word random principle. You cannot use SPACES, commas (,) or dictionary words on their own e.g. absorptiometers, Bioluminescence, daguerreotyping or xeroradiography
Examples:

- A valid password: hashspectreicons (Example password – Not to be used)
- An invalid password: Manoeuvrability

Your computer password will require updating every 365 days and you will not be able to use your last four passwords.
In the event you enter the wrong password in 5 times, your account will be locked out for 10 minutes.
All applications and information systems will be linked to your computer password, where technically possible. Where this is not possible, they will be required to match as closely as possible the Trust password policy as set out in this document.

Staff must not reuse the same passwords.
Staff must memorise their network password and not record anyway on paper or digital forms.

7.2 Email Passwords

The Trust uses the national NHS Mail system for email and has it's own password policy - https://support.nhs.net/article-categories/user-passwords/
Your password is a key component in the security of NHSmail and is required to be changed every 365 days at minimum. You will start to receive automatic email reminders from no-reply@nhs.net entitled 'your password will expire soon' 18 days prior to your password expiry. Should you not update your password within a further 90 day period from the expiry of your password, your account will be permanently deleted and the contents for your account will be irrecoverable.

8. Smartcard and Registration Authority (RA)

RA Smartcards are the primary access/token device utilised within NHS trusts to access NHS National systems.

The RA Smartcard is for use by authorised NHS Personnel who have agreed to the National Policy, Care Record guarantee, NHS Confidentiality Code of Practice and RA Terms and Conditions (T&C) and have been individually sponsored by a WAHT RA Sponsor and registered by the WAHT RA Team.

Access to Information systems via RA Smartcard should be based upon role, area of work and activities per role. Smartcards should not be shared or used to access information if the user has no legitimate reason to do so.

The RA Team monitors the use of the RA Smartcard and will report any breaches to the relevant forums as defined in the Integrated Identity Management (IIM) Process Policy. Any breaches may result in disciplinary action being taken in line with the Trust disciplinary policy.

For more information on getting, using or general help with smartcards - http://nww.worcsacute.nhs.uk/departments-a-to-z/smartcard-registration-authority-information/

9. Information and Infrastructure Management

The Digital Division shall ensure that all new information systems, applications and networks include a completed Information Security Checklist, have a recent Data Privacy Impact Assessment (DPIA) and are approved by the ICT Change Advisory Body (CAB) as part of the formal Request For Change (RFC) process before they commence operation. The Information Security Checklist provides an overview of the security requirements of the system including the steps taken to protect the data and equipment. The DPIA will detail the responsibilities of the relevant systems stakeholders, e.g. Information Asset Owners, Information Asset Administrators, users etc.

All Trust departments must involve Digital when evaluating, trialling and procuring any system that requires ICT hardware, software, support or configuration. Or if there is a requirement to implement a new clinical application, use of data stored in the digital environment or requires integration into the existing clinical applications. Digital will then ensure that all technical aspects of the system are taken into consideration before the system is implemented into the Trust digital environment. Where there is an Information Governance requirement to implement or enable use, Digital ICT will, as part of the engagement, liaise with the Information Governance team to ensure that the security of the ICT infrastructure and data is not put at risk.

To involve ICT please raise a Digital Work Request. These forms can be requested through the following email address - Wah-tr.digitalpmo@nhs.net

9.1 System Change Control

All changes to information systems, applications or ICT hardware must be reviewed and approved by the ICT CAB as part of the RFC process. This can be done by completing and submitting an RFC form. The RFC form is electronic and is located in the CAB Teams Site.

9.2 Asset Management

All Trust issued information assets are managed in accordance with Information Governance guidelines. Where staff are provided ICT assets, department managers are responsible for the local management of these assets. ICT has asset management software that will provide an inventory of equipment based on physical location and the associated software installed on that hardware device.

Departments will need to maintain an asset list for their staff to ensure that all assets are accounted for when a staff member starts with the Trust, moves within the Trust and when a staff member leaves the Trust.

If assets are transferred between departments, department managers are responsible to inform ICT to ensure that asset audit trails will be maintained.

ICT will update asset lists when equipment or software has been replaced or removed from a designated area or department.

All hardware and software components are maintained in accordance with the manufacturer's recommendation and a record of hardware and software maintenance/replacement is retained in accordance with associated support contracts and warranties.

All ICT assets will be maintained according to industry standard lifecycles. The Trust has defined the lifecycle of the following:

- Physical Server Equipment (including chassis and blades) – Five (5) to Seven (7) year replacement cycle
- Storage – Five (5) to Seven (7) year replacement cycle
- Network Devices (including firewalls) – Seven (7) year replacement cycle
- Thin Client/Zero Client Terminal – Seven (7) year replacement cycle
- PC (Including Workstations) – Four (4) year replacement cycle
- Laptop – Four (4) year replacement cycle
- Mobile Phone – Three (3) years
- Tablets – Three (3) years

9.3 Information Storage, Transfer and Disposal

The ICT infrastructure consists of endpoint devices (PCs, laptops, tablets, mobile phones, medical handheld devices, etc), some fixed location medical devices, servers, network endpoints, firewalls and other ICT reliant equipment. These devices are connected to the trust corporate network in one of two ways:

- Structured cabling
- Wireless network (Wi-Fi)

The structured cabling is present in most areas and is numbered according to location. Structured cabling is used to connect PCs, laptops (directly or by docking station), some medical devices, servers, network endpoints, firewalls and other ICT reliant equipment to the network. The wireless network is present in most Trust areas and staff have authenticated access using the Wi-Fi signal to their trust issued mobile device (laptop, tablet, mobile phone) and some wireless enabled medical devices. The access provided is to the Trust Corporate network for the delivery of patient care.

The wireless network is an extension of the physical wired network and is physically connected to a wired access point.

The Trust also provides the general public and staff with free internet access that us separate to the corporate wireless network.

9.3.1 Log Retention

The Trust is required to maintain an auditable trail of system access and information security events that are generated through system audit logs. These logs are required to support any system breaches or misuse of information.

Systems logs providing an auditable record of activity and attempted activity shall be retained for a period of 6 months. This includes operating system logs, application software logs and usage reports, network traffic logs and exception files produced during network use.

- Access to logs shall be restricted to the Digital Security Manager and IAA, IAO or SIAO of the system.
- Logs shall be securely removed when no longer required, as per the defined retention period.
- Logs shall be reviewed at an appropriate period to identify unauthorised and unusual activity patterns. Any such activity will be reported to ITSF. Where logs are voluminous it may be appropriate for the review to be done using automated software tools.
- Systems shall be appropriately sized to ensure that they have adequate capacity to accurately collect and retain logging information.
- Logs shall be appropriately backed-up and/or copied into a secure central log repository in a timely fashion. This applies particularly to client systems that are regularly re-installed.
- Log files stored on the repository shall not be able to be changed by the administrators of the systems which generate the logs.

Where logs are post-processed to extract relevant information (e.g. where the logs are too voluminous to retain in their entirety for the full retention period), they shall be reviewed before deletion of the originating log record (or the automated process will be reviewed before implementation or change) to ensure that useful information is not discarded in the process.

9.4 Corporate Network

The Trust stores and transfers information in a number of ways, across a number of electronic systems, devices and in hard copies. The Digital Division are responsible for ensuring that PII and other confidential data is kept, transferred and disposed of securely, in accordance with any legal obligations, NHS guidelines and Information Governance retention periods. Information Governance retention periods are defined by the Department of Health and associated governing bodies and can be found in the Trusts' Information Governance policies and procedures.

All data that resides within the NHS is security classified as Official for NHS staff and Official – Sensitive for patient data.

Each application solution or information system has either local direct attached storage, shared network storage or a combination of both. The data that resides in these storage locations are in restricted ICT areas, with controlled and monitored access.

Staff that require access to information can do this through their role based access and through authorisation from the system owner.

Application vendors have restricted, monitored and managed access to data relating to their application to support the application and any related incidents.

When data is transferred through the network, it is encrypted over the wireless network to its destination. When an endpoint is wired to the network, there is patch control to stop unauthorised devices being wired into the network.

All data and ICT hardware disposals are managed in accordance with the Data Protection Act 1998 and the Waste Electrical and Electronic Equipment Directive (WEEE Directive) 2012/19/EU.

9.5 Data Storage

Work related or private data (in particular sensitive data) should be not stored locally on endpoint devices. All data should be stored on a Trust file server within the correct shared drive/folder or entered into the correct application.

The storage of information is managed dynamically to enable the most used information to be prioritised over the least used information. This enables the storage to remain efficient and manage data retention, in accordance with any legal obligations - GDPR, NHS guidelines and Information Governance retention periods.

Data that is stored on smartphones or tablet devices prior to being transferred to shared files or folders is encrypted on the device and can be remotely wiped through the Trust Mobile Device Management (MDM) solution. All Trust endpoint devices including the following, but not limited to; PCs, laptops, tablets, mobile phones and USB memory sticks are encrypted to AES-256 bit.

All Trust staff with authorised access to the ICT infrastructure have a home drive (H:\). This drive is for information that staff need to access, but is not relevant to other members of their team or department. There are departmental and cross departmental shared drives that use other letters of demarcation, where information that is relevant to that team, department or other departments.

Any information that is stored in these shared drives is for shared access within the department. If it is information that forms part of a patient record, it should be input into the correct application and removed from the local endpoint device.

Should information access to the infrastructure not be available, data can be stored on a Trust issued endpoint or Trust issued encrypted USB memory stick.

9.6 Data Backups and Restore

Data stored in the Trust digital environment and associated cloud services will be backed up and retained in accordance with defined NHS Information Governance guidelines and any statutory obligations.

Backups are not encrypted, however, are stored in an application specific format and require system administrator privileges for restoration. All data is backed up and stored in a geographically separate location to the live data. Backups are initially disk to disk tasks and, where necessary, a tape archive of data backups will be taken to provide extra resilience. Data restoration of disk to disk and tape backups will be undertaken every month. The monthly restoration will be conducted on representation sample size of random backed up data to ensure the integrity of data.

9.7 Business Continuity and Disaster Recovery

The digital environment is designed to ensure that business critical applications are available. The Trust has two purpose built datacentres that are geographically separated to increase resilience. These datacentres are mains powered and have back-up generators to ensure continuity of power. Each datacentre also has Uninterruptable Power Supplies (UPS) back up for minor power outages, where the use of a generator is not required or where the generator is unavailable.

The two factors which enable the recovery of services in the Trust are the:

Recovery Time Objective (RTO) – This is the length of time taken for a solution/application/service must be restored to working order.

Recovery Point Objective (RPO) – This is the point in time, in which data can be recovered, for a solution/application/service.

The restoration of applications is managed by using the application categorisation assigned by the Trust and the RTO and RPO of categories are defined below:

Backup Classification	Datacentre Loss Recover Time	Datacentre Loss Recover Point	Application Loss RTO	Application Loss RPO	Data Capture	Infrastructure

	Objective (RTO)	Objective (RPO)				
Platinum	≥1 hr	≥1 hr	≥1 hr	≥1 hr	Replication	High availability
Gold	≥8 hrs	1 hr	≥4 hrs	1 hr	Replication	High availability
Silver	N/A	N/A	8 hrs	4 hrs	3x daily snapshot or backup	
Bronze	N/A	N/A	36 hrs	≤24 hrs	Daily backup	

Digital ICT have provided staff and clinical areas with help and guidance on their business continuity plans for planned and unplanned outages. This guidance can be found on the ICT Intranet pages - http://nww.worcsacute.nhs.uk/departments-a-to-z/acute-ict/clinical-systems-downtime-processes/

The Trust has a major incident process and it is managed by the E`PRR Manager. For more information, please go to the Intranet and go to the Emergency Preparedness section - http://nww.worcsacute.nhs.uk/departments-a-to-z/emergency-preparedness/

9.8 Infrastructure and Application Maintenance

Digital ICT will carry out planned maintenance and upgrades to the infrastructure and applications. These planned maintenance or upgrade times will be scheduled in advance and will follow the Digital change control process (RFC). Any changes that are performed by other parties or Trust divisions that affect the provision, resilience or stability of the digital environment must follow the same change control process for approval.

9.9 Application Management

The Trust ensures that all applications, information systems and other ICT products are properly licensed. All departments must involve ICT when evaluating, trialling, and procuring any information solution (hardware and/or software). Digital ICT will then ensure that all technical and Information Governance aspects of the system are taken into consideration before the system is implemented into the Trust ICT environment – DPIA process.

Digital Division manage, administer and monitor all software licenses and ensure that all information products are properly licensed. Staffs must not install software on the Trust owned property without formal, written permission from the Digital Division. Staff that breach this requirement may be subject to disciplinary action.

Applications that have been procured will follow the vendor lifecycle and will be removed if the version that is installed cannot be updated or patched by the vendor.

All applications that require databases must have a defined database structure and management schedule drafted by the supplier, agreed, managed and maintained by the Digital Division or their nominated 3rd party, to ensure that all the relevant components are optimised for performance.

Applications will be managed through Whitelisting. Where an application has been assessed and cannot be managed centrally, identified as a security risk (e.g. Teamviewer or VNC) or is not appropriate for work purposes (e.g. iTunes), these will be removed from any Trust devices and prohibited from being installed on all endpoints

9.10 Endpoint Management and Control

All Trust endpoints are centrally managed by the Digital Division. There are a number of software applications that ensure the endpoint device is secure and available for use. All endpoint devices are subject to audits (physical and remote) and may be removed, wiped or replaced if unauthorised software or hardware is installed on them.

The Trust reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act. Where persistent installation of unauthorised software or hardware is discovered, the offending user(s) will be subject to disciplinary proceedings.

Clinical or non-clinical staff members have the most secure user level implemented for daily use. Where a staff member requires additional privileges based on job role, these privileged will be documented and approved by ITSF through the Elevated Privilege Standard Operating Procedure.

Only Trust issued removable media will be permitted to be accessed on Trust endpoint devices. Digital have applied security that restricts users from transferring data to and from removable media.

9.11 Anti-Virus Procedures

All servers and endpoint devices must have approved anti-virus software installed. The anti-virus must be configured to perform regular scans and on demand scans. End point devices that are not regularly attached to the network will be subject to quarantine, where the safety and security of the device will be validated. This validation will include updating of antivirus definition files and end point scanning, before access to the Trust network can be granted. Where validation has failed, end point devices will have to have remediation actions taken before access to the Trust network is granted. This action can include complete wiping of the end point device. All Trust owned endpoints and servers are connected to the Microsoft Defender for Endpoint platform, which is provided by NHS Digital and locally managed by the Digital Division. This provides detailed information and security alerting for any malware or abnormal behaviour on Trust devices.

9.12 Bring Your Own Device (BYOD)

The Trust does not allow staff to use their personal devices for accessing locally hosted clinical information. There are a number of NHS security standards that the Trust need to achieve and maintain before a robust BYOD policy can be implemented safely, securely and reliably to ensure the confidentiality of PII and commercially sensitive information.

If staff members are required to use a device that is not issued by the Trust, this will have to be approved by the staff member’s line manager, the Digital Security Manager and the Head of Information Governance. See appendix 8. These exceptions will logged, monitored and regularly reviewed at ITSF (quarterly) and IGSG (every 6 months). Any staff member whose device is allowed to access Trust clinical information and applications, will have to maintain the same level of security and compliance as Trust issued devices. A full specification is shown in appendix 8.

9.13 Remote Access

The Trust has two general remote access solutions – ARA Portal and SSL VPN, that staff can use to access clinical applications from outside of the Trust network. Staff can request access through the NGSD portal – https://ngsd.worcsacute.nhs.uk. Access to SSL VPN is restricted for staff with Trust issued devices and is strictly prohibited for 3rd parties. All remote access solutions must use Multi-Factor Authentication (MFA). The use of internally or externally generated certificates is not a component of MFA.

10.0 Email Use and Management

The Trust uses the centrally funded NHSmail system to provide email services to their staff. The use of this email system is regulated by the policies and guidance of NHS Digital. Staff are reminded that while access to the NHSmail system is available via a standard internet connection, staff are responsible for the control of information that is stored within their email account and access to that information.

For NHSMail support issues staff can access the help section of the NHSMail website or can log an incident with the ServiceDesk through NGSD or can log a support call with the NHSMail National ServiceDesk.

Staff can access NHS mail via the Outlook application on which is provided on PCs and laptops or using the email client on any of their other endpoint devices. NHSMail has security controls that it will apply to smartphones and tablets - encryption, passcodes and other tooling, such as MFA. To request NHSMail access to be configured on your Trust issued endpoint device, please log a request on NGSD.

Further details on NHSMail policies, guidance, terms and conditions are available here - Policy – NHSmail Support

10.1 Absence

All staff who do not access their MHSMail account for 90 days will have their NHSmail account suspended.

Upon your return from absence, or should you wish to access your NHSmail account during your period of absence, you will need to contact the IT Helpdesk who will be able to un-suspend your account. They can be contacted on 0800 085 4949.

10.2 Use of Microsoft Teams

For staff using Teams, which is through the NHSMail service provision, the Trust provides controls on information security and information governance (including this policy), which set out the terms of managing of data and how staff are required to treat information, regardless of device. The MS Teams service is provided is through a 3rd party – NHSMail who have a policy framework to manage the controls required to keep information safe stored in central NHS systems. This policy supports the use of the NHSMail service and how information should be managed when using the NHSMail service.

Please ensure that this guidance is followed and any conversations, consultancy or sharing of information must be documented in the appropriate clinical or corporate solution, to ensure that there is an accurate record of conversations and changes agreed.

The Digital team have local administrator privileges to the NHSMail Teams provision. This enables the local management of the environment for staff. For further details on the use and support for Microsoft Teams please see the Digital ICT intranet site - http://nww.worcsacute.nhs.uk/departments-a-to-z/other-links/it-training/microsoft-teams/

10.3 Unacceptable Usage – Email

Sending “spam or unsolicited emails” is a breach of the NHSmail Terms and Conditions. This includes unsolicited commercial web mail, chain letters or advertisements e.g. circulating emails promoting your own business.

Staff are advised to be vigilant against hoax or unsolicited emails (Phishing) when using NHSmail. The NHS is specifically targeted by cybercriminals and there are thousands of Email hoaxes and ransomware attacks that are actively being used to gain PII, staff personal details or disrupt clinical services in the NHS environment. These types of attack vary in approach and take the guise over a range of subject matter, including:

- False claims of email account suspension
- Bank account details being compromised
- Supposedly free giveaways in exchange for forwarding emails.
- Bogus virus alerts.
- False appeals to help sick children.
- Pointless petitions that lead nowhere and accomplish nothing.
- Dire, and completely fictional, warnings about products, companies, government policies or coming events.

Digital Support staff will never ask for your password or bank details in an email.

Email addresses must not be disclosed unnecessarily. Disclosing Email addresses when filling in surveys or questionnaire will/may increase the risk of receiving unwanted junk messages.

Staff are prohibited from sending Global emails. Please contact the Trust Communications Team in the first instance where any information needs to be distributed to a large circulation for advice on the best methods.

Remember that all laws relating to written communication also apply to Emails and they could be presented as evidence in a court or tribunal.

Your emails may also be open for disclosure to anyone making a request under the Freedom of Information Act 2000 or a subject access request under the Data Protection Act 1998.

In addition users should be aware of their responsibilities to:

- Ensure that the identity of a recipient to whom they are sending an Email is correct.
- Any transmission of Personal Identifiable Information (PII) to an unauthorised and/or unsecured email system must be encrypted (see Appendix 3 for guidance on emailing PII). A list of authorised and secure email addresses is contained in Appendix 3a. For further information on NHSmail acceptable usage please follow this link – Acceptable Use Policy – NHSmail Support
- Any use of a commercial or profit making nature, or any other form of personal financial gain.

10.4 Email storage and retention

Whilst Email is not intended to be a filing system, the archiving facilities can provide a means of meeting the retention periods as detailed in the retention and disposal schedule of the Records Management Policy. Emails should be kept if they constitute a business record, note that if the information is in a document attached to the e-mail then the attachment should be saved within the normal document management system of the department (e.g. folder in the M:\ drive). Emails which need to be retained can also be stored in this way.

NHSmail has its own retention policy – NHSmail: Data Retention and Information Management Policy

The Trust has a mail archiving solution called Mailsafe. This solution stores any email that was present in the Exchange email system (pre March 2016). Staff who had a @worcsacute.nhs.uk email address will have email stored in the archiving solution. Staff who joined the Trust after this time will be able to archive emails (and retrieve emails) using the Mailsafe tool in Outlook

10.5 Out of Office Assistant

NHSmail provides an Out of Office service, which you are encouraged to use. This allows users to provide an automated response when away from work with a predefined message that may provide an alternative contact for any urgent issues. This will also provide the Out

Of Office message in Outlook and Microsoft Teams. An Out Of Office can be set in Outlook or Microsoft Teams and this is replicated to NHSMail.

10.6 Email Etiquette

Email is a powerful communication mechanism and therefore it should be used in a professional and courteous manner, in a similar vein to the written or spoken word. Take care what you write, because you do not know where copies of your Email may end up. See Appendix 3 for Good Practice Guidelines

10.7 Shared Email Facilities

NHSmail enables staff to provide delegate access to Email functions (and Calendar) to other staff. This is done on the staff member's behalf. Staff should be aware that in giving permissions to someone else they are still responsible for any Emails sent on their behalf. All Emails should therefore state that they are being sent on behalf of another. See appendix 6 for further details.

10.8 Disclaimers

All Trust emails automatically have a disclaimer attached, as per the NHSmail terms and conditions. The following is the current NHSmail disclaimer:

This message may contain confidential information. If you are not the intended recipient please:
i) inform the sender that you have received the message in error before deleting it; and
ii) do not disclose, copy or distribute information in this e-mail or take any action in relation to its content (to do so is strictly prohibited and may be unlawful).
Thank you for your co-operation.

NHSmail is the secure email, collaboration and directory service available for all NHS staff in England. NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and other accredited email services.

For more information and to find out how you can switch visit Joining NHSmail – NHSmail Support

10.9 Generic Email Accounts

Generic Email accounts require an account owner to be assigned who has overall responsibility for its maintenance, including the management of users with delegate access. Any new account needs to be requested by raising a request in the NGSD Portal – https://ngsd.worcsacute.nhs.uk

A Generic Account Request Form (Appendix 6) will also need to be completed by the account owner and their approving line manager.

10.10 Internet Email Accounts and Cloud Services and Storage

The use and access of internet email accounts and public cloud services and storage (e.g. Azure, AWS, Dropbox, Apple iCloud, Box, etc.) for PII and confidential Trust information is prohibited, unless expressly granted through the Information Governance Steering group and is in line with the Digital strategy.

The phrase "cloud storage" can be defined as any third-party solution which stores information to an online storage facility such as Google Drive, Dropbox and OneDrive.

The Trust provides cloud file storage through the OneDrive for Business environment that is managed and supported by the Trust Digital Division. Access to the OneDrive for Business service is only provided through the Trust Digital Division. The use of other cloud services without the express agreement through the Digital Division is not managed, supported or secured to the required standards and could breach NHS data regulations and GDPR.

Where necessary, systems that require the use of cloud services will be deployed for use within the Trust. Any data or system that resides within public or private cloud provisions will be governed by the same security statements outlined in this policy. The data sovereignty of information is restricted to the United Kingdom. If this is not possible, the Trust must follow NHS and central government policy to ensure the security of information stored outside of the United Kingdom.

11. Internet Management

The Trust provides internet access to assist in the delivery of patient care and the running of the Trust. ICT monitor all internet traffic and audit website access to ensure that internet access is not being used excessively or reducing the Trust’s ability to provide patient care.

Staff are able to use the internet for limited personal use during designated break times and are reminded of the following:

- Internet access is at the discretion of the Trust and if demands at particular times of the day become excessive (e.g. lunchtime), and performance of the network suffers as a result, personal use may have to be reduced or removed.
- The internet is to enable staff to access research material and other information relevant to your work
- Staff should be aware that the security of sites visited and of their personal details (name, address, financial information etc.) cannot be guaranteed since temporary files and internet page history records are often automatically retained by PCs.
- If any member of staff unintentionally connects to an inappropriate website – gambling, pornography, criminal activity or terror related site, they should inform their line manager and the Digital Service Desk immediately.

Access to internet websites and associated content is filtered and monitored. Certain categories of content have been blocked in accordance with any legal or statutory obligations, NHS guidelines and Information Governance guidelines and policies. Internet access via the Trust is also filtered, monitored and managed by Adept, who provide HSCN connectivity for the Trust under management from NHS digital for network connectivity between NHS organisations and the World Wide Web.

To engage the workforce and provide a better service to the patients of the Trust, the use of some social media sites has been approved. User access to these sites is monitored and any staff member that contravenes Trust policies while using social media at work will be subject to disciplinary action.

Unacceptable Usage – Internet

- Creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material or any data capable of being converted into obscene or indecent images or material.
- Accessing Child Pornography will result in immediate reporting of the incident to the police. **THIS IS A CRIMINAL OFFENCE**
- Creating, downloading or transmission of material that is abusive or threatening to others, serves to harass or bully others or designed to cause distress or anxiety. For example any material that discriminates on the grounds of race or ethnicity, gender, sexual orientation, disability or political or religious beliefs.
- Posting of messages on Internet message boards or other similar web-based services that would/could bring the NHS into disrepute, or contravenes confidentiality requirements, such as Facebook, Twitter, Bebo and Wikipedia; for further details please refer to Appendix 4 Guidance on Social Networking.
- Using the Internet to conduct private or freelance business for the purpose of commercial gain.
- Excessive use of the Internet for personal use
- Personal use of the Internet must be limited to official break times or outside working hours
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user's data or hardware.
- Downloading (and uploading) streaming video or audio/music for entertainment purposes.
- Accessing gambling sites
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user's data or hardware.
- Downloading (and uploading) streaming video or audio/music for entertainment purposes.
- Accessing gambling sites.
- Creating, downloading or transmitting information of a terrorist content
- Staff must reasonably understand copyright, trademark, libel, slander and public speech control laws, as not to inadvertently violate any laws which might be enforceable against the Trust. Copyright is a piece of text which accompanies a work and expresses the rights and wishes of the owner(s), you will normally need permission to use someone else's copyright work but in certain very specific situations you may not. Copyright applies to all sorts of written and recorded materials from software and the internet to drawings and photography.
- PII, confidential or sensitive information should not be entered on web-based surveys; unless it meets encryption standards; any such requirement would need Caldicott Guardian/SIRO approval.

12. Confidentiality

All users are bound by Information Governance Policies including Data Protection, Freedom of Information, Confidentiality and Information Security. Users are also bound by best practice guidance such as the Caldicott Principles and the common law duty of confidentiality. Additionally, users are not permitted to disclose confidential / sensitive information relating to any aspect of the business of the NHS.

13. Training and awareness

- This Policy will be promoted by the Digital Division, by using the Intranet, Staff communications e.g. Worcestershire Weekly, Trust Induction and briefings where the information contained is relevant to the discussion. Staff must sign the User Acceptance Declaration to confirm that they have read and understood the contents of this policy. Staff are also required to complete mandatory IG training annually.

14. Monitoring and Compliance

Page/ Section of Key Document	Key control	Checks to be carried out to confirm compliance with the Policy	How often the check will be carried out	Responsible for carrying out the check	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Page 10	Breaches in policy and incidents will be identified and reported.	Initially logged as a call via the Service Desk for evaluation and, where appropriate, an Incident being raised and investigated as per each Organisation's guidelines.	Whenever a breach in Policy or an incident occurs	Investigating officer	Reported in line with Organisation Policy through IG leads and IGSG; where appropriate being escalated in line with SIRI guidelines.	Low level breaches and Incidents will be reviewed at Organisation's IGSG 4 times a year. Serious incidents will also follow this process and are additionally included in the individual Organisation's SIC and annual report, in line with NHSD

						SIRI guidance.
page 11	breaches in access controls will be identified and reported	Initially logged as a call via the Service Desk for evaluation and, where appropriate, an Incident being raised and investigated as per each Organisation's guidelines.	Monthly	Computacenter	Reported to the ITSF forum and serious breaches will be escalated to IGSG	Summary reports will be provided quarterly and serious breached are reported at the following IGSG session
page 14	Backup and retention	check integrity of tapes, backup jobs are completed and restoration of information is possible	Tape Integrity - annually Backup Job Completion - Daily Data Restoration - Monthly	Computacenter	Reports of non conformity send to weekly operational meeting. Where data is lost, this is reported to the appropriate division and to IGSG	Annually
page 23	Antivirus	Monitor malicious code non conformities	Daily	Computacenter	Reported to the Security and Risk forum and serious breaches will be escalated to IGSG	Six monthly
Page 19	Breaches in internet usage	Proxy Server monitoring	Daily	Computacenter	Reported to the Security and Risk forum and serious breaches will be escalated to IGSG	Quarterly

15. Dissemination

This policy will be available on the Trust Intranet at all times and circulated via Trust Brief/Newsletters when amendments are made. Any key amendments to the Policy will be communicated to staff groups via Trust briefs.

16. Policy Review

This policy will be reviewed every 2 years, or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health, NHS Digital, the NHS Chief Executive and/or the Information Commissioners Office.

17. Background

Equality requirements
None - equality assessment Supporting Document 1

Financial risk assessment
None - financial risk assessment Supporting Document 2

Consultation
The following stakeholders have been consulted during the production of this policy:

- Head of Infrastructure and Cyber Security
- Computacenter Information Security Manager
- Chief Technology Officer
- Head of Enterprise Wide Applications
- Information Governance Groups at Organisation and County Level

Contribution List
This key document has been circulated to the following individuals for contributions;

Designation
Head of Infrastructure and Cyber Security
Director of IT/Chief Technology Officer
Computacenter Information Security Manager for Worcestershire Acute Hospitals NHS Trust
Chief Digital Officer
Caldicott Guardian

This key document has been circulated to the chair(s) of the following committee's for comments;

Committee
Digital Senior Management Meeting
Information Governance Steering Group
Trust Management Executive
Information Technology and Security Forum

18. Approval Process

This Policy will be approved by the relevant Committee bi-annually.

19. Version Control

This section should contain a list of key amendments made to this document each time it is reviewed.

Appendix 1
Users Responsibility Statement

The purpose of this document is to summarise the key user responsibilities and requirements for:

- ICT Services – Access and Use
- Information Security
- Internet and E-Mail Access
- Anti-Virus
- Relevant Organisation's Incident Reporting
- Access control
- Equipment Disposal
- Home working
- Code of Conduct for Employees in Respect of Confidentiality

It is your manager's responsibility to ensure that you are aware of this and other related documentation which are relevant to your role within the Organisation.

User Responsibility Declaration

I confirm that I have read and understood the content of the Information Communication and Technology Policy, which is relevant to my role. By doing this, I therefore accept responsibility for abiding by the statements within the policy throughout my working practices.

I acknowledge that wilful disregard for this policy in my actions may make me liable for action in accordance with the Trust's disciplinary procedures.

Name ___________________________________

Job Role/Title ___________________________________

Department ___________________________________

Date of Policy Acceptance ___________________________________

Signature ___________________________________

Name of Line Manager ___________________________________

By following the guidelines in this statement the users can minimise risks in relation to information security. Non-compliance may result in disciplinary action being taken in accordance with relevant Organisation's disciplinary policy, and may lead in very serious cases to dismissal for gross misconduct, as detailed in your Organisation's Code of Conduct for Employees in Respect of Confidentiality.

To obtain a copy of the disciplinary policy please discuss with your manager or the Human Resources department.

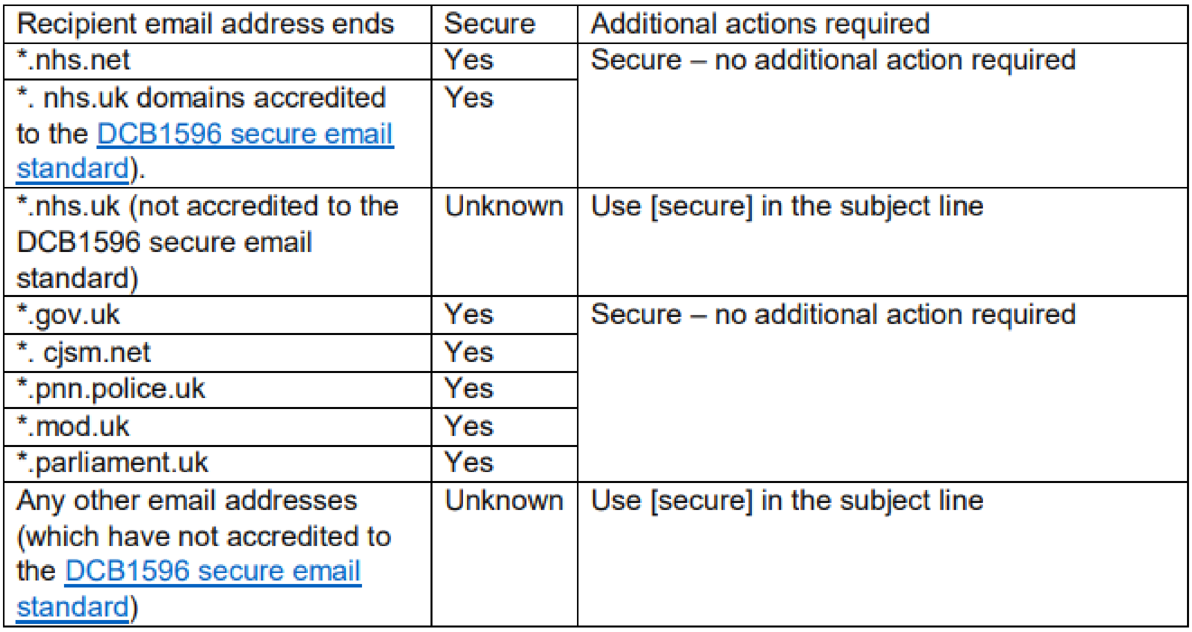
Appendix 2

Emailing Person Identifiable Information (PII)

Emailing PII is detailed in the NHS mail policies and procedures. When emailing patient information, the NHS number should ideally be used as a means of identification, where appropriate bracketing the person’s initials to confirm identity.

PII should only be emailed if it is:

(A) Emailed by NHSmail where sender and recipient addresses **both** end in nhs.net
(B) Or to the following trusted domains form nhs.net



Recipient email address ends	Secure	Additional actions required
*.nhs.net	Yes	Secure – no additional action required
*. nhs.uk domains accredited to the DCB1596 secure email standard).	Yes	
*.nhs.uk (not accredited to the DCB1596 secure email standard)	Unknown	Use [secure] in the subject line
*.gov.uk	Yes	Secure – no additional action required
*. cjsm.net	Yes	
*.pnn.police.uk	Yes	
*.mod.uk	Yes	
*.parliament.uk	Yes	
Any other email addresses (which have not accredited to the DCB1596 secure email standard)	Unknown	Use [secure] in the subject line

Further details can found about securing information in emails at the links below.

DCB1596: Secure email - NHS Digital

Sharing Sensitive Information Guide for NHSmail

Appendix 3
Good Practice Guidelines

1. Email Good Practice

- Log in regularly and respond to requests promptly
- Advise people when you are not available. When out of the office and not able to log into your mail account, use the tools within your system to notify others of your inability to read your mail
- Be selective about who receives your Emails, especially when using "Reply to All". Do all recipients need to see the reply?
- Use distribution lists with care – is it important that all addressees receive this Email?
- use Organisation-wide distribution lists only to communicate important business information that has genuine site-wide value
- Unless there has been explicit consent to share Email addresses use the Blind Carbon Copy, Bcc, option; this is particularly relevant when emailing patients, further details in Appendix 5, but may also be relevant for other external addresses.
- Check that Emails are addressed to the correct recipient when using a Global Address List.
- Check the Email before despatch. Once you have clicked the SEND button the Email cannot be retrieved once opened
- Use discretion when forwarding a long Email message to group addresses or distribution lists
- Place large attachments in a shared location (where applicable) and then send the path to the file via the Email
- Print only essential Mail
- Request an Email delivery receipt
- Request a read receipt, using message options, only on time critical mail
- Any requirement to save personal mail should be done so in a folder marked Personal

2. Email Etiquette

- Sign off with your name, Organisation and contact details
- Use the subject field with a few short descriptive words to indicate the contents when sending Emails. It will assist the recipient in prioritising opening of Emails and aids future retrieval of opened messages
- Type your messages in lower case. Using capital letters is considered aggressive
- Be careful about content. Email is easily forwarded. Do not write something in an Email that you would not write in a letter or say to someone face to face
- Maintain the conventions normally used in sending a letter by post. If you usually address someone as "Dr. Smith", do the same in Email. Emails carry the same etiquette as traditional communication; they also carry the authority of the sender!

3. Email Housekeeping

- Ensure that when the size of a mailbox approaches maximum storage limit set on your server, items are moved to a folder

- Keep the amount of Email in your inbox to a minimum. Delete Emails after reading, response or action, ensuring Deleted Items is emptied regularly. Saving messages uses valuable disk space

- Review saved Emails every month and delete the ones no longer required. If there is an Email that may be required in the future, it should be archived.

4. Issues to Avoid – Don't

- Be caught out by the speed of Email. Do not act impetuously. Is your first reaction the one you want the recipient to receive?
- Share your Email password or use other people's account to send your messages
- Send a mass mailing circular via Email
- Send Emails that may be misconstrued by the recipients
- Verbally attack in electronic form
- Send Email in upper case, this is the equivalent of shouting in someone's ear
- Send to too many people just because you can!
- Send large attachments by Email. If you believe that most recipients will print the document, try to use another method of sending the hard copy
- Send executable attachments unless essential – some intranets prohibit downloading them as Executable files cause a computer to perform tasks as opposed to a file that only contains data, so carry a higher risk of viruses

Appendix 4
Social Media – Staff must refer to the Social Media Policy

Appendix 5

Guidance around patients emailing the Trust

If your service/department uses Email as a means of contacting patients, then you have a duty to inform your patients that the information contained within the Email will not be confidential or secure and can potentially be intercepted. This is a requirement of the Data Protection Act 1998 and the NHS Code of Confidentiality 2006.

Patients should be informed:

- Exactly why their information is being collected and the ways in which their information is used. Please refer to the Organisation leaflet/poster – 'Your Information: What You Need to Know'.
- The confidentiality and security of the information in the Email cannot be guaranteed whilst in transit and that an Email should contain the minimum amount of personal information required to identify them.
- The Organisation has no control over, or responsibility for, an Email stored by a patient's own Email Service Provider e.g. Hotmail; noting that personal Email accounts are vulnerable to security breaches.
- That any agreement to share their Email address with fellow patients effectively puts their Email address in the public domain, so the Organisation no longer maintains control over who it is shared with.

Staff should also be aware that:

- The actual identity of an individual sending or receiving an Email cannot always be guaranteed; please ensure that the patient's Email address has been confirmed and is periodically verified.
- That a register needs to be maintained of Email addresses being used so that on receipt of a request to remove details this can be done efficiently and that any agreement to share Email addresses with fellow patients is recorded.
- Any requirement to send information to more than one patient in a single Email should be done via the Blind Carbon Copy, Bcc, option; unless there has been explicit consent to share Email addresses. This is of particular relevance if the Organisation holds patients Email addresses in a distribution list.
- When emailing a patient an additional disclaimer should be used as well as the standard, automated, Organisation Email disclaimer. Please see an example disclaimer below.
- Where a member of staff/service/department Email is published on the Internet that is it accompanied with a disclaimer. Please see an example disclaimer below.

Suggested additional disclaimer/footer/signature:

Please be aware that the confidentiality and security of any information exchanged via Email cannot be guaranteed and that by signing up to this service you are aware of and acknowledge the associated risks. Make sure that you always use the minimum amount of personal information needed to identify yourself and/or others (*where appropriate service to specify*). The Organisation has no control, or responsibility, over personal information stored by a person’s own Email Service Provider. Any personal information that is processed by the Organisation will be done so in accordance with the Data Protection Act 1998.

Appendix 6: Request for a Generic E-Mail Account

Generic E-Mail accounts allow more than one user to access an account; they should only be used if there is not a requirement to trace activity back to an individual. Generic accounts must have an Owner assigned; this is to be the person who takes overall control and responsibility for the account. This form needs to be completed, when requesting a new generic account or reassigning ownership, by the account owner. Requests will be considered providing the necessary control measures are in place:

Owner responsibilities

The account owner is responsible for:

- Co-ordinating the request for the generic account and obtaining the relevant line manager's authorisation.
- Deciding controlling and maintaining who has access to the generic account; this means setting up the relevant personnel with delegate access.
- Ensuring a log is maintained and retained of who has access to the Generic account and providing ICT with updated lists on a regular basis.
- Ensure ICT are kept informed of changes in requirement to the generic account by the account owner logging a request on Directa, particularly if the owner needs to be changed or the account is no longer required. Please note a new Request for a Generic Account form will need to be completed for the new named owner.
- Ensuring any use of generic email accounts for the sending/receiving of Person Identifiable Information (PII), confidential or sensitive information (PII for the purposes of this document) is in line NHSmail guidelines and adheres to the detail in the secure email diagram.
- Ensure that Caldicott approval has been obtained for any PII that leaves the trust and that the Code of Confidentiality, available from the Trust's Intranet, is adhered to.
- Ensuring that the ICT Policy and other Trust policies relating to information governance and security are adhered to.

Generic Account Agreement

This Generic E-Mail Account Request must be signed by the account owner, their line manager and where appropriate the Caldicott Guardian - this can be done electronically, providing it is sent from their respective mailboxes for audit purposes.

PRINT NAME & SIGNATURE:	
JOB TITLE:	
DEPARTMENT&LOCATION:	
CONTACT TELEPHONE NUMBER:	
DATE:	
Will PII be leaving the Trust, if so please specify?	

I Agree to the responsibilities as outlined above and:

- Are aware that the very nature of a generic account means activity cannot be attributed to an individual, thus losing the audit ability of records. Generic E-Mail should, wherever possible, be used for receiving mail and that any replies are made from an individual's mailbox.

- Failure to comply with these requirements could result in the withdrawal of the account and may lead to disciplinary action.

LINE MANAGER’S NAME & SIGNATURE:	
JOB TITLE:	
DATE:	
Direct Request Number:	

Appendix 7

Internet Mail Exemption Form

Requests for Staff Webmail Exemptions / Requests for Webmail Sites Exemptions

Form Exemption Number (formally Serial Number)	
Name of Applicant	
Username (Username for logging into your PC)	
Job Role/Title	
Department	
URL of Work Related Webmail Address to be made exempt	
Reason for Exemption	
Name of Senior Manager Approving	
Justification for Approval	
Signature of Approver	
Information Governance Approval	
ICT Security Approval	
Date of Request	

Reason for Approval/Rejection (if applicable)	
Date Exemption Actioned (to be completed by ICT/Computacenter)	

Work related Person Identifiable Information (PII) must **NOT** be included in any Webmail/Hotmail type email accounts. Any incident arising from the inappropriate transportation of PII must be reported and will be subject to Trust disciplinary procedures. Please submit completed forms on NGSD – https://ngsd.worcsacute.nhs.uk as part of an “other” requst.Email signatures from approvers are accepted.

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	Does the Policy/guidance 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	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	N/A	
4.	Is the impact of the Policy/guidance likely to be negative?	No	
5.	If so can the impact be avoided?	No	
6.	What alternatives are there to achieving the Policy/guidance without the impact?	No	
7.	Can we reduce the impact by taking different action?	No	

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, 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 Assistant Manager of Human Resources.

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	**Yes/No**
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	None

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval