IT Security Policy

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	The purpose of this policy is to ensure all Solent Staff, Contractors and third parties are aware of their responsibilities, with regards to ensure that IT requirements are always followed and adhered to
Document Type	[x] Policy
Reference Number	Solent NHST/Policy/ IT03
Version	1
Name of Approving Committees/Groups	Policy Steering Group, Clinical Executive Group
Operational Date	July 2021
Document Review Date	July 2024
Document Sponsor (Job Title)	Director of IT
Document Manager (Job Title)	Head of IT Service Delivery
Document developed in consultation with	ICT Group Information Security Group Information Governance
Intranet Location	Business Zone > Policies, SOPs and Clinical Guidelines
Website Location	FOI Publication Scheme
Keywords (for website/intranet uploading)	IT security, disposal, computer rooms, virus, IT, security, computer, network, software, hardware, data, information, media, anti-virus, anti-spam, malicious software, inappropriate use, backup, storage, connections, email, internet, portable devices, workstation, laptop, tablet, USB, encryption, confidentiality, integrity, availability, incidents, approved access, smart phone, Person Identifiable Data (PID), Security Incidents, Monitoring, logs, Policy, IT03

Amendments Summary:

Please fill the table below:

Amend No	Issued	Page	Subject	Action Date

Review Log:

Include details of when the document was last reviewed:

Version	Review Date	Lead Name	Ratification Process	Notes
1	New Policy	Mark Thomas, Technical Design Authority	Policy Steering Group, Clinical Executive Group	

SUMMARY OF POLICY

This document describes the controls and processes that have been put in place to maintain the confidentiality, integrity, and availability of information stored and processed on Solent NHS Trusts IT infrastructure.

- Password/Passphrases should never be disclosed (this includes to other staff within the trust)
- All end user devices (this means laptop, desktops, tablet) should be locked or logged off when unattended
- Staff must be cautious about opening any potential “SPAM” emails (also known as unsolicited email, sent in bulk to multiple recipients at the same time)
- Staff must be cautious about opening any potential “Phishing” emails (Phishing is a way of trying to obtain information via elicit emails) and should report such to the service desk before deleting if instructed to so at the earliest possible opportunity
- Staff are not permitted to use non-trust devices on the network without prior written approval from the IT Department
- Staff must not install any software on Trust computing equipment without prior written approval from the IT Department
- All IT equipment and applications must be used responsibly, and staff must understand the terms of acceptable usage
- All IT assets (which including equipment, software, IT configuration information and infrastructure) are Trust property and are entered on the Trust’s IT asset register maintained by the IT Department
- The disposal of redundant equipment is the responsibility of the IT Department including the secure disposal of media holding and/or having stored personal information
- All proposed changes to the Trust IT infrastructure and services (e.g. software upgrades/installations and new IT services) must be approved by the IT Department
- Staff are to comply with the General Data Protection Regulations (GDPR UK) and Caldicott Principles, never disclosing any Trust information or provide access to such information to unauthorised recipients or those who do not “Need to Know”
- Staff should expect no privacy when using the corporate network or trust resources, such use may include but is not limited to: transmission and storage of files, data, and messages
- Any member of staff observing an IT Security incident report this to the IT Service desk and then must raise a report in accordance with Incident Reporting (refer to section 17 of this document), Investigation and Learning Policy via Ulysses and provide the IT service desk with relevant details
- IT Security is an integrated part of Information Governance (IG) and all staff must undergo IG training on an annual basis
- Staff must not store personal data on the trust infrastructure (shared drives, home drive) this includes but is not limited to photographs, music and films (which may be covered by copywrite laws)

Table of Contents

Item	Contents	Page
1	INTRODUCTION AND PURPOSE	5
2	SCOPE AND DEFINITION	5
3	PROCESS	5
4	ROLES AND RESPONCIBLITIES	6
5	ACCEPTABLE USE	9
6	UNACCEPTABLE USE	10
7	ACCESS CONTROL	12
8	REMOTE ACCESS	12
9	STORAGE	13
10	CORPORATE NETWORK	13
11	PHYSICAL SECURITY	14
12	END USER DEVICES	14
13	EMAIL	15
14	IT PROCUREMENT	16
15	IT DISPOSAL	16
16	BACKUP	17
17	REPORTING INCIDENTS	17
18	REVIEW	17
19	SUCCESS CRITERIA / MONITORING THE COMPLIANCE OF THIS POLICY	17
20	REFERENCES AND LINKS TO OTHER DOCUMENTS	18
21	Glossary	18
	Appendix	
	Appendix 1 – Equality Impact Assessment	19

1. INTRODUCTION & PURPOSE

1.1 Data stored on the servers, end user devices or third-party provided solutions (such as TPP SystmOne, but not limited to) for Solent NHS Trust should be classed as critical assets and should in all cases be treated as such. Unless otherwise directed by the Information Governance Team all data should be classed as Confidential.

1.2 Compliancy with the legal and regulatory framework is mandatory, the Trust must ensure that it preserves the confidentiality and integrity of information but still enabling effective and appropriate use.

1.3 Exceptions to this policy must be approved by the Solent IT Department.

2. SCOPE & DEFINITIONS

2.1 This policy applies to all staff, locum, permanent, and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers), bank staff, Non-Executive Directors and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, agency workers, and other workers who are assigned to Solent NHS Trust.

3. PROCESS

3.1 Security of Solent's Information Technology infrastructure is critical to the provision of services which it provides to its patients and wider community and protective measures put in place, must ensure that Information Governance (IG) requirements are satisfied. Part of this process is maintaining the Confidentiality, Integrity, and Availability of Trust information. To conform to the Information Security Assurance requirements of NHS Digital's Data Security and Protection Toolkit (DSPT) Solent shall:

3.1.1 Maintain the Confidentiality of information including business, patient and staff identifiable information by protecting it in accordance with Data Protection Act, NHS Code of Practice, Caldicott, "Need to Know" Principles and other appropriate legal and regulatory framework criteria ensuring that information is only accessible by those authorised to have access.

3.1.2 Ensure the Integrity of Trust information by safeguarding the accuracy and completeness of information and processing methods.

3.1.3 Implement the necessary measures to maintain Availability of Trust information systems and services ensuring that authorised users have access to information and associated assets when required. This includes putting in place contingency measures to ensure the minimum of disruption caused to Trust information systems and services should a failure occur.

4. ROLES & RESPONSIBILITIES

4.1 Ultimately, responsibility for IT Security lays with the Chief Executive who has delegated much of this responsibility to the Senior Information Risk Officer (SIRO). The IT Department is then responsible for developing, managing and implementing IT Security policies/processes on a daily basis.

4.2 Solent ICT and its Outsource IT Partner CGI are responsible for:

- Management of all IT related assets including but not limited to hardware, software and data
- IT security in general with CGI leading on the delivery of this requirement
- Providing advice to all users regarding implementation of this policy as required
- Recording and investigating IT security related incidents
- Implementing monitoring of computer user activity in support of investigations into breaches of this policy, when and where required
- Convening and chairing ad-hoc security briefings with colleagues to address specific IT security issues, proposing amendments to policies and procedures, and discussing other key information security topics or developments where appropriate
- Conducting IT security risk assessments as appropriate for IT projects, equipment, applications and software, identifying vulnerabilities and recommending appropriate counter measures to be used as and when required
- Regularly reviewing IT security risks and advising the Trust Risk Department regarding the emergence of new threats
- Advising IT management on all aspects of IT security and forwarding recommendations for consideration
- Auditing and monitoring the erasure of data and disposal of IT equipment and media when required
- Authorising all external and remote connections to the Trust networks in accordance with the Health and Social Care Network (HSCN) Statement of Compliance (SoC)
- Authorising access to the Trust computer rooms and amendments to the Computer Room Access Control Lists
- Liaising with appropriate security staff regarding the physical security of IT work areas (including the Trust Computer Rooms), access to such areas, auditing and monitoring access to controlled areas
- Acting as the IT Technical representative for Information Governance (IG)
- Maintaining the confidentiality, integrity and availability of Trust IT systems and the data they contain
- Implementing, monitoring and, where appropriate, enforcing compliance with this policy
- Creation, deletion or disabling computer accounts, including electronic storage areas and email accounts whilst observing Trust data retention periods
- Issuing appropriate IT security documentation when required
- Managing the IT Systems Change Control process for all change requests

- Processing requests for the use of non-publicly procured hardware/software deployments within the Trust and forwarding them to the IT Department for approval to install
- Arranging collection of IT equipment and media for secure disposal
- Erasing all Trust data stored on local Hard Disk Drives or devices where required
- Processing IT incident reports on the Trusts incident management system (Ulysses) and also forwarding them to the IT Department
- Managing, implementing, auditing and monitoring information back-up schedules and process
- Invoking and conducting disaster recovery operations when required
- Controlling external connections to the Trust networks in accordance with NHS Digital Statement of Compliance
- Provision of external remote connections for authorised users
- Ensuring that only licensed, approved software is installed on Trust IT systems

4.3 The IT Security Board Committee are responsible for:

- Monitoring all aspects of IT security
- Approving, maintaining and updating this this policy
- Notifying the board of IT security risks
- Approving, maintaining and updating the IT Security Management Plan

4.4 All Information Asset Owners are responsible for:

- Understanding what information is held on the information asset (IA) for which they are responsible and understand what is added, what is removed, how information is moved, and who has access and why
- Ensure that information is fully used within the law for the public good
- Provide a written judgement of the security and use of their asset annually to support the audit process
- Understand and address risks to all the information housed on the IA by process and/or technical measures

4.5 The People Services Department is responsible for:

- Ensuring that, as part of their contract of employment, new staff agree to the Trust's Data Protection Compliance Policy
- Ensuring that, as part of their contract of employment, new staff agree to the Trust monitoring user activity

4.6 Line Managers are responsible for:

- Ensuring that all staff under their management who use Trust computers for work purposes, plus all external users of Trust computers under their management, are aware of this and associated policies & procedures and their responsibilities outlined within them
- Ensuring account creation (for new staff) and cessation forms (or electronic equivalents) for all staff who leave the Trust are submitted to the IT Department in a timely manner
- Ensuring that IT are notified when staff move within the trust and no longer need access to departmental data

- Ensuring they inform the IT service desk where a member of their staff proceed on any type of leave of absence from the department for a period that exceeds 3 months
- Ensuring they inform the IT when a member of their staff leave the trust
- Ensuring that any departmental IT process conforms to both the Trust's Data Protection Compliance Policy and IT Security Policy and where necessary conducting a risk assessment of the process
- Ensuring that all new and current users plus all external users of Sensitive Electronic Data under their management, are aware of this and associated policies & procedures and confirm their awareness of, and adherence too
- Apply the Improving and Managing Conduct Policy when breaches occur

4.7 All Trust staff, without exception, must:

- Abide by this and associated policies & procedures and
- Report any IT security incident in accordance with the Trust's incident reporting process and also inform their line manager and the IT Department. Failure to adhere, will initiate the Improving and Managing Conduct Policy, which could result in dismissal
- Change their assigned password after successfully logging on for the first time or if a compromise is suspected
- Not allow others to utilise or 'share' their individual user accounts for any purpose. Where there may be a clear identified need for a 'shared' account this should be discussed with the IT Department and, if approved, a shared user account will be created
- Never disclose their individual account password to anyone, including other Trust computer account holders. The only exception to this may be during telephone support provided by the IT service desk when the user's password may rarely be called for under exceptional circumstances. If this occurs, the user must change their password on completion of the telephone support
- Not connect any privately procured hardware to any Trust computing equipment or network without prior written approval from the IT Department
- Not install or attempt to install any software on Trust computing equipment without prior written approval from the IT Department
- Comply with the General Data Protection Regulations (GDPR UK) and Caldicott Principles, never disclosing any Trust information or provide access to such information to unauthorised recipients or those who do not "Need to Know"
- Not access, view and/or extract any Trust information stored on Trust IT Systems for personal reasons or attempt such action, e.g. accessing clinical records of relatives and/or friends or for 'idle' curiosity
- Lock or log off if leaving any workstation unattended. If the user is using a shared workstation, they should log off rather than lock the workstation. If anticipating an absence of 30 minutes or more the individual user account must be logged off or the machine shut down
- If the workstation is not being used for a prolonged period (i.e. overnight, weekends, etc.) then it should be shut down, this gives the benefit of power

saving and also allows the completion of installs/updates that may have been deployed remotely and are awaiting a reboot

- Dispose of all computer equipment, output and media, e.g. print outs, floppy disks, CD ROM discs, USB Flash Sticks in accordance with this policy

5. ACCEPTABLE USE

5.1 **Across the Trust, the following is considered acceptable use and is not prohibited:**

- All work related to the day to day business requirements of Solent
- Conduct research within the bounds of appropriate and ethical professional behaviour
- Upgrade professional development skills (training, e-learning, professional body certification, and maintenance)
- Collaborate with work-related professional contacts and participate in discussion groups on subjects of professional interest
- Conduct internal and client work-related business with email and Internet, using common sense and ensuring proper email content when sending and receiving work-related emails
- Use emails and Internet browsing in a manner that does not interfere with other business activities, disrupt services, or incur additional costs to the Solent

5.2 Personal use of internet is acceptable. Internet facilities should primarily be used for Trust and partner agency business. However, staff may use the internet for occasional personal use at the discretion of their manager provided:

- It does not interfere with Trust work
- It is not related to a private business interest or to employment with another employer (partner agency work is permitted for staff in integrated teams). Any such breach could be referred to Human Resources and the Local Counter Fraud Specialist for further investigation and/or consideration of criminal action in line with the Managing Conflict of Interest Policy and Counter Fraud, Bribery and Corruption Policy.
- Any use for personal commercial purposes, including the sale or purchase of goods and services, makes no reference to the Trust
- It complies with this policy, including its provisions regarding misuse

5.3 Staff wishing to spend significant time outside working hours using the internet on Trust devices – for example, for study purposes – should obtain their manager's approval. It is the manager's responsibility to record and file the approval appropriately and to copy the approval to the member of staff.

5.4 The IT Department will monitor internet use from all computers and devices connected to the Solent network. For all traffic the monitoring system will record the source Internet Protocol (IP) address, the date, time, protocol and the destination site or server. Where possible, the system will record the user ID of the person or account initiating the traffic. Internet Use records will be preserved for 12 months and made available in accordance with Regulation of Investigatory Powers Act (RIPA) 2000.

6. UNACCEPTABLE USE

6.1 All facilities must be used responsibly. Staff must not misuse them by taking any action which could bring the Trust into disrepute, interfere with the Trust's work or jeopardise the security of data, networks, equipment or software

6.2 **Across the Trust, the following is strictly prohibited:**

- Trust IT networks being used to convey, share or store indecent and/or profane material on any Trust machine, or removable media storage device
- If illegal material is accessed on the internet, sent or received by e-mail, or handled via any other electronic communication the Trust may inform the police and/or the Trusts Counter Fraud Specialist and criminal prosecution may follow
- Processing any privately owned information and storing it on Trust computer equipment without the express permission of the IT Department
- Using Trust or privately procured removable media to import data to Trust networks without using the Anti-Virus scanning software beforehand
- Removing covers from any Trust IT equipment for any purposes including changing or adding components
- Adding/Installing IT equipment to the Trust networks without prior written approval from the IT Department
- Leaving workstations logged-on whilst unattended
- Installing or attempting to install any software including privately owned software onto Trust IT equipment without prior written approval from the IT Department
- Entering Trust IT Communications Rooms without obtaining prior approval from the IT Department
- Permitting others to access your individual computer account, even if they themselves are authorised Trust account holders
- Users must not deliberately misrepresent themselves or represent other users nor the Trust
- Attempt to access systems for which they have no legitimate right and may only access systems for which they are authorised to do so and for a legitimate business reason
- Use the Trust IT infrastructure to support private commercial activity including 'hosting' web sites or conduct any form of non-Trust business using Trust equipment and resources
- Connect any peripheral devices (with the exception of USB memory sticks) to Trust IT systems without the prior approval of the IT Department. Such devices include Mobile Phones, Personal Digital Assistants (PDAs), mp3 players and external hard disk drives
- Connecting personal mobile phones to any equipment for the purpose of battery charging or upload/downloading of data

6.3 The internet is an area that can be misused and this may include, but is not limited to accessing, viewing, disseminating, downloading, printing or similar actions in respect of:

- Creation, use, transmission or encouragement of material which is offensive, defamatory or infringes another person's copyright
- Pornography/adult material
- Discrimination, harassment, libellous statements
- Transmission of unsolicited commercial or advertising material
- Transmission of personal data in contravention of the law or associated policies
- Unauthorised disclosure of confidential information, especially personal data, in contravention of the law, NHS regulations or Trust policies
- Obtaining unauthorised access to the Trust or another organisation's IT facilities
- Using non-work-related chatrooms, social networks or similar services
- Games software, except for the purpose of authorised training, is not permitted for use on the organisation's equipment via web access nor may it be downloaded and installed. Authorised training software includes "games" shipped as part of the computer's operating system
- Disrupting other users' work in any way, including by viruses or data corruption
- Expressing personal views in such a way that they are likely to be interpreted as being the official policy/view held by the Trust
- Committing the Trust to purchasing or acquiring goods or services without proper authorisation
- Downloading copyrighted or confidential information without proper authorisation
- Online gaming and gambling
- Wasting network and staff resources

6.4 The Trust reserves the right to bar access to websites deemed offensive in the terms of this policy – e.g.

- Adult/sexually explicit material
- Advertisements and pop-ups
- Chat and instant messaging
- Gambling
- Hacking
- Illegal drugs
- Intimate apparel and swimwear
- Peer to peer file sharing
- Personals and dating
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and offensive content
- violence, intolerance, discrimination, hate and extremist material

7. ACCESS CONTROL

7.1 "Access Control" is a key requirement to control access to trust assets, the controls restrict access to Solent machines and many applications by requiring a logon for authentication. Typically, this is an assigned "User Identity (UserID)" and password issued by the IT service desk. System managers must determine what controls to apply for permitting users the appropriate level of access.

7.2 User Accounts are created and managed in accordance with the IT Departments internal Account Policy and Standards (Network, Computer and Applications). Line managers are responsible for:

- Requesting that the IT Department creates computer accounts for new staff before they take up their employment with the Trust via the appropriate process
- Informing the IT Service desk of those leaving their employment and providing adequate notice, at least 2 weeks in advance, thus initiating the cessation procedure using "MyIT"
- Arranging for the issue or return of any smart cards or other system identity tokens
- Notifying the IT Service desk promptly of a user's prolonged absence of three months, or longer in which case their computer accounts will be disabled (note that IT will also monitor the usage of all user accounts and will routinely disable those that have not been used for a period of 60 days whether)
- When accounts are closed, any data held within the account including Email, folders, and files will be deleted after having been archived for a period of:
- 6 months on ceasing to be employed by the Trust
- The system will not provide help messages during log-on
- The system restricts any incorrect log-on attempts to five, recording each event
- Following five unsuccessful log-on attempts, the account is disabled for a period
- Initial passwords changed by the user after first successful log-on
- Users accounts locked after 5 unsuccessful attempts to logon

8. REMOTE ACCESS

8.1 A secure VPN solution is installed on all Solent Laptop end user devices for Remote Access, all staff must ensure that when using VPN that:

- It is only to be accessed by authorised users
- Should not be used on non-Solent devices such as personal home computers
- Remote access on non-Solent devices should utilise the "Solent-Remote" Windows Virtual Desktop infrastructure. This is a secure cloud-based solution that requires a Solent user account and two-factor authentication to access. Instructions on using the solution can be obtained from the IT Service Desk

8.2 Third-party remote access requirements must be requested via the IT Service Desk with user details and business requirements.

9. STORAGE

9.1 Data should not be stored on the local hard drive of machines except in the cached User Profile. As a default position all data should be stored on network drives (e.g. R.Drive, T.Drive, G.Drive, etc…), Sharepoint or the user personal drive (One Drive).

9.2 Restricted storage is available to all users to store business related documents and other information. Access to the restricted drive locations is approved by the folder "Owner" of the restricted data. Requests for access to restricted data should be requested from the IT Service desk, by the "Owner"

9.3 Each user account has "home drive" (One Drive) storage allocated for personal work-related documents (where access should be restricted to the individual only).

9.4 Clinical data should be stored within Clinical Electronic Patient Record (EPR) application (such as, but not limited to SystmOne, Inform, R4, IaPTUS, etc…) and only within restricted drives by exception, where necessary and approved by the services Information Asset Owner.

9.5 No personal non work-related data should be stored on any of the Trust's Network storage, this specifically relates but is not limited to:

- Music
- Personal holiday photographs
- Films/Video recordings
- Sexually explicit material
- Software
- Other copyright material

9.6 Exceptions to this must be approved by the Solent IT Department and the Information Governance Team.

10. CORPORATE NETWORKING

10.1 The management of Solent's computer networks is the responsibility of the IT Department and the Trust's ICT Contractors. The controls, standards and processes used to ensure the network remains both secure and resilient are detailed on the Network Security Policy.

10.2 No unauthorised computer hardware is to be connected to the corporate network without written permission from the IT Department, this includes but is not limited to:

- Routers
- Switches
- Hubs
- Personal Laptops
- Personal Desktops
- Printers

- Wireless Access Points

10.3 Access to the Corporate Wireless network is only permitted by authorised Solent end user devices.

10.4 External connections in/out of the Trust computer networks, supporting Trust services, are subject to the rules set by NHS Digital in their Statement of Compliance (SoC) criteria. Anyone requiring an external connection, either for support of services or extended business activities, must contact the IT Department.

10.5 For Third-Party access to the Trusts network/hosting environment please contact the IT Department via the IT Service Desk with details and business requirements.

11. PHYSICAL SECURITY

11.1 **Securing offices -** Any Trust office accommodation, ward areas and support units, equipped with computer workstations used for processing Trust information, must:

- If practicable, be locked when left unoccupied
- Keep computer workstations locked using Ctrl Alt Delete or logged off if left unattended, in ward areas, the user may have to log off in order to prevent other users being locked out
- Observe the "Last Person Out" routine, checking all windows and doors are locked

11.2 **Computer Workstations -** Rules for the physical protection of Trust computer workstations/laptops are in place to help protect Trust information and safeguard the "Need to Know" principle. Users must remain alert to unusual or suspicious activity and be prepared to challenge the presence of unidentified individuals in the vicinity. If you suspect tampering with a computer workstation or unjustified presence of individuals, you must report it to Trust Security immediately (see Policy for Security and Management of Violence and Aggression).

11.3 **Mobile devices** - Including Laptops, tablets and mobile phones are not to be left unattended in public areas or left in vehicle except in a secured boot space. They are not to be left in vehicles overnight for any reason. When at home, these devices are to be stored in a secure location, out of reach from others, to protect against damage, loss or theft.

12. END USER DEVICES (ALL STAFF)

12.1 All end user devices are the property of the trust.

12.2 All end user devices must be encrypted to safeguard the data stored on the device before being issued. It is the responsibility of the Trust's ICT Contractors to ensure that no device is issued, without encryption being enabled on the device.

12.3 All end user devices must have the ability and must have installed anti-virus software before being issued. It is the responsibility of the Trust's ICT Contractors to ensure that no device is issued, without anti-virus being enabled on the device.

12.4 All users are expected to look after their allocated devices and take reasonable precautions to protect them from damage. Should an end user device become damaged it is the responsibility of the user to notify the IT Service Desk of the damage. Users may be charged should the damage be found to have been maliciously caused.

12.5 Laptops, tablets and mobile phones are the responsibility of the users that they have been allocated to, users must make all reasonable efforts to protect the devices from being lost or stolen.

12.6 Should an end user device be lost or stolen it is the responsibility of the user the devices have been allocated to, to notify the IT Service Desk so that an IT incident can be raised.

12.7 All end user devices must be returned to the IT Department when no longer required, this includes when a staff member leave.

12.8 All end user devices will be deactivated if they haven't communicated with the trusts network after 3 weeks, this is a security measure to protect the trust should a device go missing. Where a device is deactivated the user will be required to contact the IT Service Desk (0345 605 1334) for it to be reenabled.

12.9 All end user devices will be permanently removed if they haven't communicated with the trusts network after 7 weeks.

12.10 End user devices should not be used outside of the UK unless prior approval is given by IT Security.

13. EMAIL

13.1 Email must be used responsibly, and staff must understand the terms of acceptable usage Staff are to comply with the General Data Protection Regulations (GDPR UK) and Caldicott Principles, never disclosing any Trust information or provide access to such information to unauthorised recipients or those who do not "Need to Know".

- Staff should ensure that they are aware, that corporate email accounts are the ownership of Solent NHS Trust and therefore can be accessed by either ICT Department or HR (if approved by the Trust's Data Protection Officer and where there is a legitimate need), such use may include but is not limited to: transmission and storage of files, data, and messages
- Any member of staff observing an email incident (such as but not limited to SPAM, suspicious emails, etc…) must report this to the IT Service desk and then must raise an incident report in accordance with the Trust Risk Management Process (i.e. via Ulysses). Staff are to provide the IT service desk with relevant details (refer to section 17 of this document)
- Corporate email is not to be used for personal communications, all communications become the ownership of the Trust
- The security of Solent's email infrastructure is critical to the provision of services which it provides to its patients and wider community and protective measures put in place, must ensure that Information Governance (IG) requirements are satisfied. Part of this process is maintaining the Confidentiality, Integrity, and

Availability of Trust information. To conform to the Information Security Assurance requirements of NHS Digital's DSPT Solent shall:

- Maintain the Confidentiality of information including business, patient and staff identifiable information by protecting it in accordance with Data Protection Act, NHS Code of Practice, Caldicott, "Need to Know" Principles and other appropriate legal and regulatory framework criteria ensuring that information is only accessible by those authorised to have access
- Ensure the Integrity of email by safeguarding the accuracy and completeness of information and processing methods

13.2 Although IT makes every endeavour to block Spam and Phishing emails inevitable some will still get through, if an email looks to be a spam or phishing email users should:

- Notify the IT Service desk
- Do not open the email
- Do not forward the email unless instructed by IT
- Delete the email

13.3 If you receive an e-mail that contains libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions you must promptly notify Your Manager.

13.4 If you receive an e-mail that you consider having been illegally sent or illegal in its content you must promptly contact the IT Service Desk and not forward to any further recipient.

14. IT PROCUREMENT

14.1 All IT procurement should follow the Trust Procurement Policy for further information, this can be found on the intranet site "SOLNET".

14.2 Only Solent IT pre-approved software, licensing and hardware can be procured and used on the Solent network. Any purchases that do not meet these requirements will be removed and reviewed before being reinstate, should anything fail the review process it will be disposed of in line with the and disposal process.

15. IT DISPOSAL

15.1 Disposal of redundant equipment is the responsibility of the IT Department and anyone disposing of redundant computer equipment such as, monitors, workstations, keyboards, printers, etc., must contact the IT service desk to arrange for collection and disposal in accordance with the Waste from Electrical and Electronic Equipment regulations (WEEE).

15.2 All disposal of IT equipment that is capable of storing data must be securely "wiped" to safeguard this data. Just deleting the data is not sufficient.

15.3 Line managers must ensure that such equipment is not:

- Transferred outside of the Trust
- Sold or donated to charitable organisations without prior approval from the IT Department

- Storing any Trust information that has not been transferred to an approved data storage area

15.4 The status of equipment and devices that are disposed of must be updated on the asset register (please refer to the IT Asset Management Policy).

16. BACKUP

16.1 IT Department and the Trust's IT Contractors are responsible for backing up trust data stored on the server infrastructure. IT **do not** backup data stored locally on individual devices.

16.2 Backups are created on magnetic tapes which are stored off site from the data centre when not in use.

16.3 A full back is completed weekly as well as 6 incremental daily backups.

17. REPORTING INCIDENTS

17.1 All IT security incidents should be reported to the CGI Service Desk (0345 605 1334) immediately.

17.2 Information Governance should also be notified of any IT security related incidents that has, or potential has caused a data breach (refer to Data Protection Compliance Policy for details)

17.3 All incidents should be reported in accordance with the Trust Risk Management Process (i.e. via Ulysses)

18. REVIEW

18.1 This document may be reviewed at any time at the request of either staff side or management but will automatically be reviewed 1 year from initial approval and thereafter on an annual basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review or a significate Cyber/Security incident occurs internally or externally to the Trust which could impact the organisation.

19. SUCCESS CRITERIA / MONITORING THE COMPLIANCE OF THIS POLICY

19.1 Undertake audit reports and monitoring as a result of alerted suspicious activity. Such reports will be approved by Head of IT Service Delivery

19.2 Individual staff within both the ICT Department and the Trust's external ICT Contract provider(s), will be assigned responsibility to monitor key aspects of this policy and will be overseen by the Information Security Committee

19.3 The Information Security Committee will oversee the monitoring and reporting associated with this policy and report to the SIRO any risks and / or areas of non-compliance

19.4 Overall compliance will be monitored through the assessment and submission of the DSPT, which will also be audited by the Trust's Internal auditors

20. REFERENCES AND LINKS TO OTHER DOCUMENTS

20.1 Policies:

- Improving and Managing Conduct Policy
- Incident Reporting, Investigation and Learning Policy
- Data Protection Compliance Policy
- Policy for Security and Management of Violence and Aggression
- Local Counter Fraud, Bribery and Corruption Policy

20.2 Other Documents:

21. Glossary

	Explanation
GDPR UK	General Data Protection Regulations
HSCN	Health and Social Care Network
SPAM	Unsolicited Email
Phishing	Unsolicited Email trying to gain personal information
Ulysses	Incident Management System
SIRO	Senior Responsible
SoC	Statement of Compliance
IG	Information Governance
SOLNET	Solent NHS Trust Intranet
IA	Information Asset
PDA	Personal Digital Assistants
RIPA	Regulation of Investigatory Powers Act
MyIT	CGI Service Request Portal
EPR	Electronic Patient Record
WEEE	Waste from Electrical and Electronic Equipment

APPENDIX 1

Equality Analysis and Equality Impact Assessment

Equality Analysis is a way of considering the potential impact on different groups protected from discrimination by the Equality Act 2010. It is a legal requirement that places a duty on public sector organisations (The Public Sector Equality Duty) to integrate consideration of Equality, Diversity and Inclusion into their day-to-day business. The Equality Duty has 3 aims, it requires public bodies to have due regard to the need to:

- **eliminate unlawful discrimination**, harassment, victimisation and other conduct prohibited by the Equality Act of 2010;
- **advance equality of opportunity** between people who share a protected characteristic and people who do not;
- **foster good relations** between people who share a protected characteristic and people who do not.

Equality Impact Assessment (EIA) is a tool for examining the main functions and policies of an organisation to see whether they have the potential to affect people differently. Their purpose is to identify and address existing or potential inequalities, resulting from policy and practice development. Ideally, EIAs should cover all the strands of diversity and Inclusion. It will help us better understand its functions and the way decisions are made by:

- **considering the current situation**
- **deciding the aims and intended outcomes of a function or policy**
- **considering what evidence there is to support the decision and identifying any gaps**
- **ensuring it is an informed decision**

Equality Impact Assessment (EIA)

Step 1: Scoping and Identifying the Aims

Service Line / Department	ICT	
Title of Change:	IT Security Policy	
What are you completing this EIA for? (Please select):	Policy	*(If other please specify here)*
What are the main aims / objectives of the changes	Implement and define IT Security for all staff members, partner organisations and third-parties that utilise Solent NHS IT resource in any way	

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document / policy on patients in the drop-down box below. If there is no impact, please select "not applicable":

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	Not applicable	Action to address negative impact: *(e.g. adjustment to the policy)*
Sex			Not Applicable	
Gender reassignment			Not Applicable	
Disability			Not Applicable	
Age			Not Applicable	
Sexual Orientation			Not Applicable	
Pregnancy and maternity			Not Applicable	
Marriage and civil partnership			Not Applicable	
Religion or belief			Not Applicable	
Race			Not Applicable	

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, service users, carers or other voluntary sector groups?)	No	The IT security policy is required to safeguard Solent NHS trust, its staff and most importantly patient data and information. The policy has been written based on considerations taken from the IT Security Policies of Solent's STP partner trusts
Have you taken into consideration any regulations, professional standards?	Yes	GDPR UK and Data protection legislation

Step 3: Review, Risk and Action Plans

	Low	Medium	High
How would you rate the overall level of impact / risk to the organisation if no action taken?	■	☐	☐
What action needs to be taken to reduce or eliminate the negative impact?	None		
Who will be responsible for monitoring and regular review of the document / policy?	ICT		

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:	Mark Thomas	Date:	14/04/2021

Additional guidance

Protected characteristic		Who to Consider	Example issues to consider	Further guidance
1.	Disability	A person has a disability if they have a physical or mental impairment which has a substantial and long term effect on that person's ability to carry out normal day today activities. Includes mobility, sight, speech and language, mental health, HIV, multiple sclerosis, cancer	• Accessibility • Communication formats (visual & auditory) • Reasonable adjustments. • Vulnerable to harassment and hate crime.	Further guidance can be sought from: Solent Disability Resource Group
2.	Sex	A man or woman	• Caring responsibilities • Domestic Violence • Equal pay • Under (over) representation	Further guidance can be sought from: Solent HR Team
3	Race	Refers to an individual or group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.	• Communication • Language • Cultural traditions • Customs • Harassment and hate crime • "Romany Gypsies and Irish Travellers", are protected from discrimination under the 'Race' protected characteristic	Further guidance can be sought from: BAME Resource Group
4	Age	Refers to a person belonging to a particular age range of ages (e.g., 18–30-year-olds) Equality Act legislation defines age as 18 years and above	• Assumptions based on the age range • Capabilities & experience • Access to services technology skills/knowledge	Further guidance can be sought from: Solent HR Team
5	Gender Reassignment	"The expression of gender characteristics that are not stereotypically associated with ones sex at birth" World Professional Association Transgender Health 2011	• Tran's people should be accommodated according to their presentation, the way they dress, the name or pronouns that they currently use.	Further guidance can be sought from: Solent LGBT+ Resource Group
6	Sexual Orientation	Whether a person's attraction is towards their own sex, the opposite sex or both sexes.	• Lifestyle • Family • Partners • Vulnerable to harassment and hate crime	Further guidance can be sought from: Solent LGBT+ Resource Group
7	Religion and/or belief	Religion has the meaning usually given to it but belief includes religious and philosophical beliefs, including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition. (Excludes political beliefs)	• Disrespect and lack of awareness • Religious significance dates/events • Space for worship or reflection	Further guidance can be sought from: Solent Multi-Faith Resource Group Solent Chaplain
8	Marriage	Marriage has the same effect in relation to	• Pensions	Further

		same sex couples as it has in relation to opposite sex couples under English law.	• Childcare • Flexible working • Adoption leave	guidance can be sought from: Solent HR Team
9	Pregnancy and Maternity	Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In non-work context, protection against maternity discrimination is for 26 weeks after giving birth.	• Employment rights during pregnancy and post pregnancy • Treating a woman unfavourably because she is breastfeeding • Childcare responsibilities • Flexibility	Further guidance can be sought from: Solent HR team