NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Acceptable Use (IT) Policy

OFFICIALSENSITIVE: COMMERCIAL	
Policy Number	**IT/Pol/003**
Target Audience	**All Bridgewater Staff and Contractors**
Approving Committee	**Corporate Clinical Policy Group**
Date First Approved	**September 2015**
Last Full Review Date	**December 2020**
Next Full Review Date	**December 2023**
Policy Author	**Head of IT**
Version Number	**3.0**

Applicable Statutory, Legal or National Best Practice Requirements	ISO/IEC 27001, Code of Practice for Information Security Management Information Commissioner's Office (2018) Guide to the General Data Protection Regulation Computer Misuse Act (1990) Freedom of Information Act (2000) Regulation of Investigatory Powers Act (2000) Human Rights Act (1998) Equality Act (2010) Data Protection Act (2018) Regulation of Investigatory Powers Act (2000)

The Trust is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
1.0	July 2015 September 2015 September 2015	Policy Approval Group Keith Greatorex Dorian Williams	Minor amendments required Amendments completed as requested by PAG Chair approval given.
2	October 2017 Nov 2017 November 2017	Policy Approval Group J. Hogan S. Arkwright	Approved subject to minor amendments Amendments complete Approved by chair action
2.1	May 2018	J. Hogan	Minor amendments to the AUP in Sections 3, 5.1 and 7.3
2.2	May 2018	S. Arkwright	Approved by chair action
2.3	Oct 2020	M. Corkery	Comments made
2.4	Nov 2020	J. Hogan	Reviewed
2.5	Nov 2020	DIGIT	Sign-off agreed
2.6	December 20	Corporate Clinical Policy Group	Approved subject to minor amendments and final chair approval
2.7	Dec 2020	James Hogan	Minor amendments completed
3.0	Dec 2020	S. Arkwright	Approved by chair action

Does this policy impact/potentially impact on: • **Staff** • **Patients** • **Family Members** • **Carers** • **Communities**	**Yes**	**Please contact the Trust's Equality & Inclusion Manager at:** **Email: ruth.besford@nhs.net**
	No	**Please sign and date below:** **Name: J A Hogan** **Email Address: james.hogan1@nhs.net** **Date: 27/10/20**

Education & Professional Development Question

In order to ensure that any training requirements are discussed and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements.

Please answer the following question by entering a cross in the box below:

	Yes	No
Does this document have any additional training requirements or implications?		X

If you have answered **YES** you must forward a copy of this document to Education & Professional Development **before** submitting to the Policy Officer.

Date submitted to Educations & Professional Development: ……

No further action is required if you have answered NO.

Contents

1 Introduction

Information and information systems are important assets and it is essential to take all the necessary steps to ensure that they are protected at all times, additionally, to ensure that the systems are available and accurate to support the operation and continued success of Bridgewater Community Healthcare NHS Trust (hereafter the Trust). The Trust acknowledges that we must demonstrate our commitment to, and delivery of, effective information security.

The aim of the Trusts policies, standards and guidelines is to maintain the quality, confidentiality, and availability of information stored, processed and communicated by and within the Trust.

These policies, standards and guidelines are used as part of the Information Security Management System (ISMS) within the Trust.

To facilitate effective working the Trust allows all 'employees' access to appropriate information systems and technology, including the internet, and email. However, with this access brings risk to the Trust. This policy, therefore, sets out the standards applicable for the use of information and information systems within the Trust.

1.1 Objective

The purpose of this policy is to define the accepted practices and responsibilities associated with the correct usage of Trust information systems. These systems include physical devices/items and logical applications/software plus all associated information.

1.2 Scope

This policy applies to all Trust staff, whether permanent, part-time or temporary with responsibilities listed within section 5. It also applies to contractors granted access to Trust information and information systems.

Any staff from other organisations working on the Trust infrastructure are required to understand and abide by this policy.

2 Definitions

The definitions applicable to this policy are as follows:

Acceptable Use – describes the supported and approved usage of Trust information and information systems.

3 Abbreviations

The abbreviations applicable to this policy are as follows:

SIRO Senior Information Risk Owner

ISM	Information Security Manager
ISMS	Information Security Management System
IT	Information Technology
IG	Information Governance
RIPA	Regulation of Investigatory Powers Act
USB	Universal Serial Bus
PID	Patient Identifiable Data
HSCN	Health and Social
DSPT	Data Security and Protection Toolkit
IM&T	Information Management and Technology
ICO	Information Commissioners Office

4 Other Relevant Procedural Documents

This policy should be read in conjunction with the following documents:

Information Governance Policy

Information Security Policy

Mandatory Training and Induction Policy

Network Security Policy

Home Based Working Policy & Procedures

Mobile Computing Policy

Risk Management Framework

Incident Reporting Policy

Leavers Policy

Safe Haven Policy

Disciplinary Policy and Procedures

Dignity and Respect at Work Policy

Social Media Policy

Data Protection Policy

Mandatory Training and Induction Policy

Anti-Fraud, Bribery & Corruption Policy

Access Control Policy

Freedom of Information and Environment Information Regulations Policy

Subject Access / Access to Health Records Policy

Video Consultation Procedure

WhatsApp for Communications including Video Calling – Coronavirus (COVID-19) Pandemic Temporary Procedure

PANDO Messaging Application for use in Trust Services Guideline

5 Roles and Responsibilities

5.1 Senior Information Risk Owner (SIRO)

The Lead Director with overall responsibility for this document is the Director of Finance, Information and Performance who is also the Senior Information Risk Owner (SIRO).

The SIRO is conversant with and has overall responsibility for Information Risk Management in the Trust and for monitoring compliance with the Information Security Policy.

The SIRO is responsible for:

- Reporting to the Board on information risks following assurance from the Information Asset Owners.
- Reporting to the Quality and Safety Committee on information risks and through the Statement of Internal Controls following assurance from the Information Asset Owners. The SIRO is the Director of Finance.

5.2 The Caldicott Guardian

The Caldicott Guardian is the Chief Nurse and is responsible for:

- Ensuring that the organisation conforms to the Caldicott Principles, NHS Confidentiality Code of Practice and Information Governance Standards and Data Protection Act
- Monitoring the investigation and resulting actions of security breaches
- Guiding the organisation on Confidentiality and Data Protection issues.

5.3 Data Protection Officer

The Data Protection Officer (DPO) for the Trust is held by the Trust Secretary.

The DPO reports directly to the Board about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

With the support of their office, the DPO will:

- Provide advice to the organisation and its employees on compliance obligations with data protection law
- Advise on when data protection impact assessments are required
- Monitor compliance with data protection law and organisational policies in relation to data protection law
- Co-operate with, and be the first point of contact for the Information Commissioner
- Be the first point of contact within the organisation for all data protection matters
- Be available to be contacted directly by data subjects
- Take into account information risk when performing the above.

5.4 Information Security Manager

The ISM is responsible for:

- Maintaining and reviewing the policy
- Taking operational responsibility for implementing and managing related procedures to this policy
- Examining the functionality and secure nature of any required applications, using official framework guidance and established usage evidence to determine risk and suitability
- Establishing secure baseline configurations and appropriate controls and to maintain these, commissioning regular 3rd party audits
- Monitoring and reporting on any security breaches or system failures and reporting to Digital Information Governance & Information Technology Group (DIGIT)
- Maintain and routinely review an up to date and accurate register of IT risks on the Trust Risk Register on Ulysses

- Contacting the Trust's Anti-Fraud Specialist (AFS) immediately in all cases where there is a suspicion that Trust IT is being used for fraudulent purposes in accordance with the Computer Misuse Act 1990. The ISM will also liaise closely with the AFS to ensure that a subject's access (both physical and electronic) to Trust IT resources is suspended or removed where an investigation identifies that it is appropriate to do so.

5.5 IT Staff

All staff in IT Services must comply with the contents of this policy. IT staff will:

- Establish secure systems, maintain the confidentiality, integrity and authenticity of information held within managed electronic systems

- Adhere to standards and establish operational procedures to support this policy ensuring that all regulatory, contractual and legal requirements are complied with

- Provide support, advice and guidance to enable users to adequately protect devices and information

- Ensure compliance with the core components of the standards in the Data Security and Protection Toolkit (DSPT) to protect information assets to deliver confidential, accurate and timely information to support patient care and associated support operations

- Ensure that all managed systems are controlled and protected against unauthorised access

- Ensure that IT assets purchased are identified, classified and protected as required

- Establish and maintain business continuity planning processes to ensure that serviceability and the integrity of information are maintained

5.6 Information Asset Owners

Information Asset Owners (IAOs) will:

- Lead and foster a culture that values, protects and uses information for the benefit of patients

- Know what information comprises or is associated with their asset(s) and understand the nature and justification of information flows to and from the asset

- Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy

- Understand and address risks to the asset and provide assurance to the SIRO

- Ensure there is a legal basis for processing and for any disclosures and refer queries about any of the above to the Information Governance team

- Ensure all information assets they are owner for are recorded on the Information Asset Register and maintained

- Undertake specialist information asset training as required.

5.7 Digital Information Governance & Information Technology Group

The DIGIT group will monitor compliance with this policy on behalf of the Trust, and will report on the management and accountability arrangement for Information Governance (IG), and provide assurance to the Board through the Trusts sub committees.

5.8 All Managers

All managers are responsible for:

- Ensuring that the policy and its supporting standards and guidelines are embedded fully into local processes and that there is on-going compliance and reporting of any untoward incidents or risks.

Managers are also responsible for ensuring that their permanent, temporary staff and contractors are aware of:

- The Information Security policy and related policies

- Their responsibilities for the security of electronic systems

- How to access advice on information security matters

- The security of the physical environment

- How to report breaches or potential breaches of system or environment security through the organisations reporting procedures

- For ensuring that all staff are made aware of this policy.

5.9 System Users/All Staff

All System Users must comply with security procedures including the maintenance of data confidentiality and data integrity and of the operational security of the systems that they use.

Users must be aware (general awareness should be established during staff induction and periodically updated via mandatory IG training, staff bulletins, desktop messages and global messages etc.) that:

- All suspected or actual virus infection or functionality issues should be reported to their relevant IT Help Desk who will escalate as appropriate

- There are operational security requirements of the information systems they use and they must comply with those requirements to ensure the confidentiality, integrity and availability of the information in that system is maintained to the highest standard

- They must protect the managed assets by safeguarding user names and passwords and/or smart cards that have been issued to them

- Access to systems is automatically logged; and any activity will be attributed to the username

- Audits are undertaken by IM&T to identify and investigate failed or inappropriate logins

- Audits are undertaken to identify any misuse of systems or failure to adhere to this or any other Trust policy

- There are restrictions imposed on the transmission, copying, or reproduction of patient identifiable information from the managed system

- The Trust is fully committed to the Data Protection legislation, NHS: Confidentiality Code of Practice and the Caldicott Principles regarding the protection and use of personal information.

6 Equipment

- Trust information systems

- Data Security and Protection Toolkit

7 IT Equipment and the Network

7.1 Context

The Trust has an established Network which permeates all areas of the organisation sites allowing user access to Information Technology (IT) Systems and information in order to allow them to do their jobs effectively.

7.2 Business Use

IT access is provided on the basis of business need. Use of any equipment provided for business purposes is acceptable only where such use falls within the normal day to day remit of the individual.

In particular, the following user obligations must be applied:

- Users must not in any way cause damage to the Trust's IT Systems

- Users must adhere to the terms and conditions of all license agreements relating to IT Systems, which they use. This includes software, equipment, services documentation and other goods

- Users must not modify any software nor incorporate any part of the provided software into their own work without permission from the designated authority

- Users must not load any software onto the IT Systems without gaining express permission from the Information Security Manager

- Users must not deliberately introduce any virus, for example worm, trojan horse or other harmful or nuisance program or file, onto any IT Systems, nor take deliberate action to circumvent any precautions taken or prescribed by the Trust to prevent this

- Users must not delete or amend the data or data structures of other users without their permission

- Users must not, in their use of IT systems, exceed the terms of their registration. In particular they must not connect to any other computing IT systems without the permission of the designated authority

- Users of networks and remote IT systems shall obey any published rules for their use

- Users must ensure that they start and terminate each session of use of IT systems in accordance with published instructions

- Users must not interfere with the use by others of the IT systems; they must not remove or interfere with output belonging to another user

- The creation, display, production or circulation of offensive material in any form or medium is forbidden

- Users must take every precaution to avoid damage to equipment caused by smoking, eating or drinking in its vicinity. In particular, eating or drinking in IT system rooms is forbidden

- Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT systems

- Users must not share login details and passwords with any other user or write them down where they could viewed and by another person and used to gain system access

- All users must ensure their workstation is locked whenever it is not in use.

7.3 Personal Use

Equipment and systems access are provided for users' business purposes. Personal use represents an area of concern and inevitably increases the Trust's risk exposure. Therefore, any personal usage should be kept to a minimum and take place within agreed work breaks. Also this usage should at all times be within the constraints of Trust policy and procedure.

Some examples of unacceptable use could include the storage of illicit, pornographic or racist material or the use of the equipment to duplicate copyrighted materials such as software or music.

Users must not install personal software on Trust equipment regardless of its nature. Only software, which supports Trust business, is to be installed and in all instances this must be done by a member of the IT Department. In all instances, usage can only be acceptable if it is by a Trust employee/ contractor. Use of equipment by family or friends is unacceptable regardless of the purpose of use.

All Patient Identifiable Information should be stored on either an encrypted device (USB pen etc.) or preferably a secure server. Under no circumstances should Patient Identifiable Information be moved or transmitted by non-secure Email or un-encrypted media/devices.

Agile and Mobile users/workers should also make themselves aware or the following key policies:

- Home Based Working Policies and Procedures
- Mobile Computing Policy

8 Email

8.1 Context

Email is an essential business tool, facilitating the sharing and dissemination of information between staff and beyond organisational boundaries. While essential to the effective operation of the Trust there are risks to its use as has been demonstrated in highly publicised cases in the media.

Email sent over the Internet is not secure and as such Patient Identifiable Data (PID) should never be sent in this form (for exceptions see 7.3 NHS Mail).

Under no circumstances should Patient Identifiable Information be transmitted by non-secure Email. The Data protection policy applies and should be followed when transmitting patient identifiable data.

8.2 Business Use - Email System

The Trusts Email system is, essentially, a business facility. Users should be aware that Email is legally attributable to the Trust in exactly the same way as letters/fax/memos and therefore information, which could be construed as legally binding.

The Freedom of Information and Environment Information Regulations Policy and/or the Subject Access / Access to Health Records Policy has more detail.

The content of all Email stored on equipment owned by the Trust remains the property of the Trust at all times. Users should not have an expectation of privacy in anything they create, store, send or receive on their computer.

The Trust has the capability and right to monitor emails if there are suspicions of inappropriate or none acceptable use in alignment to this or any other Trust policy. Misuse of email or any other Trust system may be dealt with by way of the Disciplinary Policy and Procedure.

By default, a disclaimer is added to every individual's Email as follows:

All Emails leaving the Trust are virus scanned. The recipient(s) should make their own anti-virus provision.

"This Email may contain confidential and/or proprietary information some or all of which may be legally privileged and is for the intended recipient(s) only. Please notify the author by return if this Email has been sent in error or misdirected to you and destroy any copies. You must not, disclose, distribute, copy, or print this Email or any attachments if you are not the intended recipient.

The information contained in this email and your reply, may become available to the public under the Freedom of Information Act (2000), unless legally exempt from disclosure."

Users are responsible for managing their own mailboxes and ensuring that messages, which are no longer required, are deleted. Users should be aware that sending large attachments affects the performance of the network and as such any attachments in excess of 20Mb should not be sent via Email.

IT Services provide a secure file transfer service to facilitate the transmission of large data sizes.

To aid users, a number of key email 'do's and 'don't' are set out in appendix A.

8.3 NHS Mail

The Trust, like all other NHS organisations, has subscribed to the NHS directory service. As part of this, NHS Mail accounts can be established for all staff.

NHS Mail is a secure internet mail, calendar and directory service within which every employee has an "address for life" which is always @nhs.net and does not change as they move organisations. It is also available directly from the internet allowing users to access their mail from any location. This is in addition to the Trust account given to users on request.

Transfer of personal information by email should be avoided unless the information is encrypted i.e. transmitted in a coded format.

NHSmail is the only British Medical Association and Department of Health approved email service for securely exchanging clinical data between email users. Therefore, email should not be used for sending confidential information unless both sender and recipient are using an NHSmail account.

Non-NHS domains that are secure for the transmission of sensitive data are listed below and have the following suffixes (address after the '@' sign):

- secure.nhs.uk
- gov.uk
- pnn.police.uk
- cjsm.net
- mod.uk
- parliament.uk

All information that contains PID (staff or patients) needs to be handled securely at all times.

Once you have an NHS.net account:

When sending emails outside of NHSmail if the domain is not trusted use **[secure]** at the start of the email **subject**. [Secure] this is not case sensitive.

If any user believes that PID cannot be transferred by NHS Mail or has any doubts about the security of an e-mail they must contact the Information Governance Department.

8.4 Internet Mail

Messages sent using commercial internet mail accounts such as:

- Yahoo
- Hotmail
- Google

Are particularly insecure and staff may not use them from the Trusts computing equipment.

8.5 Personal Use

It is the Trusts view that limited personal use is acceptable but such usage should not interfere with the performance of your job, therefore use of Email facilities for personal purposes should be confined to non-working hours. Non-working hours can be defined as time outside of a shift, i.e. allocated breaks including meal breaks.

Further, such use should only be for personal purposes and should not be to support or pursue private businesses.

Users should be particularly careful regarding the content of emails; examples of areas of possible concern are listed below:

- Jokes
- Images

- Religion
- Sexism
- Race
- Nationality
- Culture
- Gender
- Transgender
- Sexual Orientation
- Age
- Disability
- Ethnicity
- Derogatory comments
- Personal attacks
- Diversity
- Comments with the potential to cause business reputational damage

<u>The list is not comprehensive and a sense of political correctness should be maintained at all times.</u>

In particular, users should ensure that:

- Personal use is kept to a level that is not detrimental to the main purposes for which the accounts were provided
- Priority is given to the use of accounts for business purpose
- Personal use must not be for commercial purposes or any form of personal financial gain
- Personal use must concur with the Trust policies and procedures
- Personal use must not conflict with any of the users obligations as an employee of the Trust

9 The Internet

9.1 Context

The Internet is a valuable tool for research and distribution of information. However, the risk associated with connection to and use of the internet is extreme and requires significant management and control.

The Trust provides internet access to all staff via a managed HSCN (N3) connection, which is a secured service, which aims to protect the NHS from many of the risks associated with the Internet.

Users must not install or configure any connections to commercial Internet service providers. Such connections are insecure and may, in certain circumstances, represent a breach of the Trusts HSCN statement of compliance, which could result in the Trust being disconnected from HSCN.

Users should also note that internet usage is tracked and logs are retained that can be produced as evidence in the event of any accusations of misuse.

9.2 Business Use

Internet access is seen as a key facility in enabling users to perform their jobs. Access to all business specific websites is supported and any non-business websites where content is deemed to be acceptable, general conditions detailed in 8.3 below.

9.3 Personal Use

It is the Trusts view that limited personal use is acceptable but such usage should not interfere with the performance of your job, therefore use of the Internet for personal purposes should be confined to non-working hours. Non-working hours can be defined as time outside of a shift for example allocated breaks including meal breaks.

At all times there are a range of conditions that should be applied to such access:

- Users must not use streaming media services such as 'YouTube' for personal reasons. This type of service is extremely resource intensive and should only be used to convey work related information. Overuse of streaming media services may have a knock-on detrimental effect on the quality and availability of the online working environment of all Trust users

- Users must not access, download or transmit any obscene, indecent or pornographic images, data or other material

- Users must not access, download or transmit any defamatory, sexist, racist or otherwise offensive images, data or other material

- Users must not access, download or transmit any copyrighted material in a manner that violates that copyright

- Users must not access, download or transmit any material that is designed or likely to annoy, harass, bully or inconvenience other people

- Users must not access, download or transmit material created for the purpose of corrupting or destroying the data of other users

- Users must not allow non-Trust persons access to systems

- Use must be for personal purposes and not for the support of any private business ventures.

Such guidance does not represent the totality of possible inappropriate access; users should be aware at all times that the principles of decency and legality will be applied. A simple rule of thumb could be described as “if the material could cause offence to even one individual then it is probably inappropriate.”

The final “decision” on the appropriateness of material accessed will lie with the Trust. It is the Trusts view that limited personal use is acceptable (except for streaming media services) but this should be confined to non-business hours and should, at all times, be legal. Further, such use should only be for personal purposes.

The use of Trust equipment to support or pursue private businesses is not acceptable.

9.4 Unacceptable Types of Sites

This policy does not contain advice to staff on the inappropriateness of certain types of sites/content, it merely advises users to stay within ‘acceptable’ boundaries appropriate to their role and the organisations standing.

Access to a blocked site can be granted upon request to IT Service Desk. If the request is deemed against policy it must be supported by a management approved business case and any required risk assessment. The case will then be reviewed at DIGIT with a view to sanctioning access.

10 Telephony

All telecoms services and facilities provided by the Trust for its employees are there to support the business of the Trust, abuse of these facilities is a breach of this policy, some of our telephone systems have the facility have the capacity to record conversations (see section 11.2).All calls should be for business use though the Trust acknowledges there maybe exceptions.

The following are examples rather than a comprehensive list of those exceptions

- The call is related to a personal emergency

- It is a legitimate call to the emergency services

- Calls agreed with line management.

The following conditions though not comprehensive are also considered best practice:

- Any incoming personal calls should be kept short in length and infrequent
- Any agreed outgoing calls must be kept short in length and be infrequent
- Receipt of text messages is discouraged as these can be distracting to patients and colleagues.

Specifically, the following situations should always be avoided:

- Providing a Trust telephone number as a contact point in personal advertisements in the press, on the internet etc.
- Premium rate phone numbers must not be called such as those associated with competition lines, racing lines, chat rooms etc.
- Transmission of any offensive material in either voice, text or image format from Trust supplied mobile phones
- Use of Trust telephony for personal use outside of business hours.

11 Office Communicator and Instant Text Based Services

11.1 Context

- You must not use any instant messenger service to cause any annoyance, inconvenience or anxiety to others
- You must not use the service to impersonate someone else
- You must not make statements that are defamatory to or misrepresent others
- Defamatory postings may include but are not limited to postings which harm the personal or business reputation of another or exposes them to hatred, contempt or ridicule, or lowers them in the estimation of their community or deters other people from associating or dealing with them
- You must not use the service to distribute illegal material or material that you did not create, unless you have the permission of the owner of the relevant rights to that material
- You must not use the service to transfer files that contain viruses, trojans or any other harmful programs.

12 Compliance

12.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this policy standard.

12.2 Review and Monitoring

The Trust has in place routines and tools to regularly audit compliance with this and other Trust policies and standards. The Trust proactively audits users to monitor compliance and investigate any allegations of misuse, including potential offence(s) under the Computer Misuse Act 1990.

Under section 1 of the Computer Misuse Act 1990, a person is guilty of an offence if he or she causes a computer to perform any function with intent to secure access to any program or data held in any computer; the access he or she intends to secure is unauthorised; and he or she knows at the time when he or she causes the computer to perform the function that this is the case.

The maximum penalty for offences under the Computer Misuse Act 1990 is 12 months' imprisonment and/ or a fine under summary conviction and two years' imprisonment and/ or a fine on conviction on indictment.

Any evidence of system misuse may result in system or service access withdrawal and result in subsequent disciplinary action.

In the event that it is suspected that Trust IT is being used for fraudulent purposes in accordance with the Computer Misuse Act 1990, the matter will be referred to the Trust's Anti-Fraud Specialist (AFS) and/ or the police.

In exceptional circumstances The Regulation of Investigatory Powers Act (2000) (RIPA) 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.

In addition, communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of the Trusts business, and the employee’s position within the Trust.

Any monitoring will be undertaken in accordance with the above Act and the Human Rights Act (1998).

13 Reporting Security Incidents

If any person becomes aware that there has been inappropriate use of equipment, email, the internet etc. they should report this via the Service Desk hosted online form 'IG Request'. All staff must ensure that incidents and near miss events are also reported to the Risk Management Team via relevant incident reporting procedures.

In the event of an incident that is considered to be a HIGH or EXTREME risk, that this is communicated immediately to the Assistant Director of IT or designated lead in their absence as this will require direct escalation to the SIRO and/or Executive Lead, along with the Risk Management Team and IG team who will report to the ICO if needed in compliance with the organisations Incident Reporting Policy.

14 Disciplinary

Any Users or Employees who are deemed to be breach of this policy may be subject to disciplinary proceedings as per the Trusts Disciplinary Policy.

15 Consultation

Key individuals/groups involved in the development of the policy to ensure it is fit for purpose once approved.

Name	**Designation**
Nick Gallagher	Director of Finance, Information and Performance
Dave Smith	Assistant Director of IT
Alan Tweddell	Head of IT
Sharon Ramsdale	Information Governance & Records Manager
Paul Dwerryhouse	Service Delivery Manager / Service Desk Manager
Mary Corkery	Policy Officer
DIGIT	
Phillip Leong	Anti-Fraud Specialist
Corporate Clinical Policy Group	

16 Dissemination and Implementation

16.1 Dissemination

The Information Security Manager will disseminate this policy to all staff via the Team Brief. The policy will be made available on the Trust intranet (The Hub) and published in the bulletin.

It is imperative all staff and other stakeholders who will be affected by this document are proactively made aware of any accepted changes in practice that may mean this policy requires amendment.

16.2 Implementation

Appropriate on the job learning via annual mandatory IG training (data protection awareness level 1) plus cyber security advisories will aligned to peer group review help provide managers with the knowledge to support the implementation of this policy.

General awareness will be established during staff induction and periodically updated via mandatory IG training, staff bulletins, desktop messages and global messages.

17 Process for Monitoring Compliance and Effectiveness

Any issues of non-compliance (which may be identified via human or technical report or automated alert) will be raised and addressed by the Information Security team.

Reporting of incidents will be reviewed and monitored through the risk management process.

18 Standards/Key Performance Indicators

- Standards in the DSPT.
- Audits are undertaken by IM&T to identify and investigate failed or inappropriate logins.
- Audits are undertaken to identify any misuse of systems or failure to adhere to this or any other Trust policy.
- Establishing secure baseline configurations and appropriate controls and to maintain these, commissioning regular 3rd party audits.

19 References

Computer Misuse Act 1990, c.18 [online]. Available at: http://www.legislation.gov.uk/ukpga/1990/18/contents

Data Protection Act 2018, c.12 [online]. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents

Equality Act 2010, c. 15 [online]. Available at: http://www.legislation.gov.uk/ukpga/2010/15/contents

Freedom of Information Act 2000, c.36 [online]. Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents

Human Rights Act 1998, c. 42 [online]. Available at: http://www.legislation.gov.uk/ukpga/1998/42/contents

Information Commissioner's Office (2018) Guide to the General Data Protection Regulation (GDPR) [online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf found here https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

ISO/IEC 27001, Code of Practice for Information Security Management https://www.iso.org/isoiec-27001-information-security.html

Regulation of Investigatory Powers Act 2000, c.23 [online]. Available at: http://www.legislation.gov.uk/ukpga/2000/23

Bridgewater Community Healthcare NHS Foundation Trust

Email Do and Do Not List

Do	Do Not
• Think carefully when composing Emails, the nature of Email is that it is often less formal than letters etc. This informality can cause differences in interpretation amongst recipients • Use distribution lists appropriately. Is it important that all addressees receive this Email? • Check your Emails regularly, and respond to requests promptly • Advise people when you are not available by setting 'Out of office auto-reply' on the system • Be selective about who receives your Emails, especially when using 'Reply to All'. Do all recipients need to see the reply? • Remember that a message from a Trust Email account reflects on the organisation. It is also admissible in a court of law and may require disclosure under the Freedom of Information Act • Manage your mailbox • Keep your password secure • Mark emails as private or confidential, where appropriate • <u>Ask if you are in doubt</u>	• Send patient identifiable information by Email unless utilising an approved secure email system • Send offensive, pornographic or illegal messages or material • Use the Email accounts of others except where proxy rights have been granted • Send global messages, except for alerts • Send messages to those whom you are aware do not wish to receive the mail • Use the account of another individual without official access to that account. • Use the Email system for personal gain • Forward junk mail, spam or chain mail • Send attachments in excess of 20Mb • Open mail where you do not recognise the sender or the contents appears to be dubious – it may be a virus • Open attachments with exe, vbs, ps1,psm1 and psd1 extensions • Be caught out by the speed of Email. Think carefully, is your first reaction really the one that you want the recipient to receive.