Acceptable Use Policy

Owner: Simon Hassall

Version: 2.5.0

Hertfordshire, Bedfordshire, and Luton ICT Shared Services is hosted by Hertfordshire and West Essex Integrated Care Board

Copyright

Document Control

Document Owner	S Hassall	**Approved by**	HBL ICT SMT
Document Author(s)	A McLaren, S Hassall	**Date of Approval**	14th November 2023
Version	2.5.0	**Date for Review**	12 Months

Version Control

Version	Status	Commentary	Date	Author
0.0.1	Draft	Initial document based on the NHS Digital Acceptable Use policy and includes relevant sections from the Email and Internet Policy, which was retired following the move to NHSMail	Sept 2018	A McLaren
1.0.0	Live	Confirmed by SMT 24//9/2018	24/9/2018	A McLaren
1.1.0	Live	Additional section 3.2.2 on Criminal Penalties. Confirmed by P Turnock 1/10/2018	28/9/2018	A McLaren
1.1.1	Draft	Additional changes for ENHCCG following review: Replace “Trust” with “Organisation” Remove “Social networking” as an example of a site that contains information that is inappropriate, offensive or unlawful as this is now legitimately used by teams Remove “NHS laptops shall never be (via cable or wireless) directly connected to other non NHS IT equipment or systems; as homeworking using secure Broadband has been agreed Additional information on use of PCD from NHS Digital website	16/11/2018	A McLaren

		Clarification 3.3 regarding changes to restrictions for team use Typing errors amended		
1.2.0	Live	Confirmed by P Turnock	6/12/2018	A McLaren
1.2.1	Draft	Annual Review: 1: Remove elements of Example Policy 3.3 Variations roles of authorizers in organisation included 3.5.1 clarification of eating and drinking in the vicinity of IT equipment 3.3 Restrictions on Internet Sites moved to section 4.4 References updated	Oct 2019	A McLaren
2.0.0	Live	Authorized at SMT	4/11/2019	A McLaren
2.0.1	Draft	Annual review (alignment of core policies Title amendment (Head of Technical Services to Associate Director) Update to versions of related documents	Aug 2020	A McLaren
2.1.0	Live	Authorized at SMT	1/9/2020	A McLaren
2.1.1	Draft	Update to 3.4.2 amend first bullet to correct as “when left unattended” : Update to Implementation plan replacing IG Toolkit with DSPT and the updated training level 1	Oct 2020	A McLaren
2.2.0	Live	Authorized at SMT	3/11/2020	A McLaren
2.2.1	Draft	Annual Review amendments - role titles	Nov 2021	A McLaren
2.3.0	Live	Authorized at SMT	16/11/2021	A McLaren
2.3.1	Draft	Annual review Document template/format updated CCG references updated to ICB HBL ICT Department names updated Internal reference - Document names updated External reference – Reference to EU legislation removed. GDPR changed UKGDPR	Oct 2022	S Hassall
2.4.0	Live	Authorised by HBL ICT SMT	8/11/2022	S Hassall
2.4.1	Draft	Annual review HBL ICT job title and department name updates References to NHS Digital updated to NHS England Document owner updated HWE ICB modifications– Reference to Counter Fraud, Bribery and Corruption Policy in Internal Reference section. Edit	September 2023	S Hassall

		to Section 5 Point 7. Edit to Section 3.3. Point 11.		
2.5.0	Live	Authorised by HBL ICT SMT	14/11/2023	S Hassall

Terms and Acronyms

Term	Definition
EU	European Union
ICT	Information and Communications Technology

Terminology

Term	Meaning/Application
SHALL	This term is used to state a Mandatory requirement of this policy
SHOULD	This term is used to state a Recommended requirement of this policy
MAY	This term is used to state an Optional requirement

Implementation Plan

Development and Consultation	Hertfordshire, Bedfordshire and Luton ICT Shared Services (HBL ICT) is committed to the fair treatment of all, regardless of age, colour, disability, ethnicity, gender, gender reassignment, nationality, race, religion or belief, responsibility for dependents, sexual orientation, trade union membership or non-membership, working patterns or any other personal characteristic This policy / procedure will be implemented consistently regardless of any such factors and all will be treated with dignity and respect. To this end, an equality impact assessment has been completed on this policy.
Dissemination	Staff can access this policy via the Intranet and will be notified of new/ revised versions via the staff briefing. This policy will be included in the ICB's Publication Scheme in compliance with the Freedom of Information Act (FOI) 2000
Training	All staff members are required to carry out the mandatory IG training through the NHS Data Security Training (Level 1)
Monitoring	3rd Party Audit, Data Security and Protection Toolkit (DSPT), spot check
Review	The policy will be reviewed annually
Equality, Diversity and Privacy	Completed separately

References

External : Legislation, Guidance and Standards	All applicable UK legislation including but not limited to: ♦ Data Protection Act (2018) and UK GDPR (2018) ♦ Computer Misuse Act (1990) ♦ Freedom of Information Act (2000) ♦ Health and Social Care (Safety & Quality) Act (2015) ♦ Environmental Information Regulations (2004) ♦ Access to Health Records Act (1990) ♦ Human Rights Act (1998) ♦ Regulation of Investigatory Powers Act (2000) Department of Health and NHS Regulations and Guidance including but not limited to: ♦ NHS Digital Acceptable Use Example Policy (v1.0, 2017) ♦ NHSMail Policies, Acceptable Use Policy v3 September 2018 ♦ DSPT Big Picture Guide 1 ♦ Guide to Confidentiality in Health and Social Care (2013) ♦ NHS Statement of Compliance v6.0
Internal : Related Documentation	♦ Information Security Policy ♦ Mobile Device Security Policy ♦ Telecoms Policy ▪ Records Management & Information Lifecycle Management Policy (which includes Data Quality) (HWE ICB) ▪ Counter Fraud, Bribery and Corruption Policy (HWE ICB) ♦ Information Governance Strategy ♦ Management of Records Policy and Procedure ♦ Data Quality Policy ♦ Incident Policy ♦ Confidentiality Policy
Enclosures	none

Contents

1 Executive Summary 8

2 Scope 8

3 Use of Information Systems 8

3.1 Authorised Users 8

3.2 Unauthorised Information Access 8

3.3 Misuse of Information Systems 9

3.4 Criminal penalties 10

3.5 Access and Disclosure of Electronic Communications 11

3.5.1 General Provisions 11

3.6 Monitoring Communications 11

3.6.1 Inspection and Disclosure of Communications 12

3.6.2 Special Procedures for Monitoring and Disclosure 12

3.7 Guidelines for IT Equipment Use 12

3.7.1 Physical Protection 12

3.7.2 General Use 13

4 Internet Acceptable Use 14

4.1 Restrictions on Internet Sites 14

5 NHS Email Acceptable Use 15

6 Disciplinary Action 15

Appendix A. Comment Form 16

1 Executive Summary

This policy sets out the commitment of the organisation to preserve the confidentiality, integrity and availability of communications and to ensure that these are effectively and lawfully managed.

2 Scope

- All staff employed by the organisation, contractors, seconded staff from other organisations and any other persons used by the organisation or engaged on the organisations business
- All locations from which the organisations IT services can be accessed
- Variation to some parts of the policy may be allowed where local conditions do not permit full implementation. Applications for such variation must be made to HBL ICT Associate Director of Digital Solutions and approved by the HBL ICT Managing Director or Associate Director, to ensure the security of shared infrastructure and to ensure meeting Information Security requirements, and should the assessed level of risk warrant it, the Stakeholder Board before being introduced.
- All staff are expected to use NHSMail for email communications, following the move from the local legacy email exchange system in 2018. Policy and Acceptable Use of NHSMail is found on NHS Digital website

3 Use of Information Systems

3.1 Authorised Users

Staff will be given a username and/or a smartcard and a password to access the systems they are authorised to use. These will identify the user to the system.

Contractors and other persons working on behalf of the Organisation may be given authority to use these services in accordance with the Partner's policies and subject to appropriate authorisation.

The use of any email and internet resources must be related to the legitimate business activity of the organisation. This includes authorised professional and academic pursuit.

3.2 Unauthorised Information Access

- The organisation and third party employees **shall** only be authorised access to information relevant to their work.

- Accessing or attempting to gain access to unauthorised information **shall** be deemed a disciplinary offence.
- When access to information is authorised, the individual user **shall** ensure the confidentiality and integrity of the information is upheld, and to observe adequate protection of the information according to NHS policies as well as legal and statutory requirements. This includes the protection of information against access by unauthorised persons.

3.3 Misuse of Information Systems

- Use of NHS information systems for malicious purposes **shall** be deemed a disciplinary offence. This includes but is not limited to:
  - Penetration attempts (“hacking” or “cracking”) of external or internal systems.
  - Use of another person’s identity (username/password or smartcard) to access services
  - Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic.
  - Discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.
  - Acquisition or proliferation of pornographic or material identified as offensive or criminal.
  - Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software.
  - Storage or transmission of large data volumes for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads.
- Users accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other person without a legitimate purpose and prior authorisation from senior management is strictly forbidden and **shall** be deemed a disciplinary offence.
- Use of NHS information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and **shall** be deemed a disciplinary offence.
- Personal use that creates a cost or inconvenience for the organisation

- Intercepting or opening electronic files addressed to another recipient without their permission (except for authorised employees in the course of the organisations business)
- Use of electronic systems to harass or intimidate others or to interfere with the ability of others to conduct the organisations business
- Downloading of any files that could jeopardise the security and integrity of the organisations networks or systems
- Injudicious use of work time and facilities for private purposes
- Sending and receiving of NHS related information other than in compliance with this policy
- If identified misuse is considered a criminal offence, criminal charges **shall** be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.

3.4 Criminal penalties

All staff **should** be aware that misuse of personal data is a criminal offence. The following is not intended to be a comprehensive list of all applicable legislation, but as a guide to the most common offences. Staff who have any concerns about these offences, should contact their local Data Protection Officer for advice.

Data Protection Act 2018:

Section 170 Unlawfully obtaining personal data.

It is an offence to knowingly or recklessly obtain or access personal data without the permission of the Organisation. This includes accessing patient or staff records without a clinical or business need.

Section 171 Re-identification of de-identified personal data

It is an offence to knowingly or recklessly re-identify data that has been anonymised, without the permission of the Organisation.

Section 173 Alteration or deletion of personal data to prevent disclosure to the data subject.

Once a person has made a request to access their records, it is an offence to alter, delete or damage that record to prevent it being released. Staff should be mindful that any record they create relating to an individual (staff or service user) can be disclosed to that person. This includes emails, health records, handwritten notes, and recorded messages (ie Dictation).

Freedom of Information Act 2000:

Section 77 Altering or deleting records to prevent disclosure.

Environmental Information Regulations 2004:

Section 19 Altering or deleting records to prevent disclosure

Similarly, it is an offence to alter, delete or damage records to prevent release once they have been requested under the Freedom of Information Act or Environmental Information Regulations.

Computer Misuse Act 1990:

Section 1 Unauthorised access to computer material

Section 3 Unauthorised access with intent to impair, or with recklessness as to impairing, operation of a computer

Section 3ZA Unauthorised access causing, or risking, serious harm.

Section 3a Making, supplying or obtaining articles for use in an offence under Section 1, 3, or 3ZA)

3.5 Access and Disclosure of Electronic Communications

3.5.1 General Provisions

To the extent permitted by law, the organisation reserves the right to access and disclose the contents of any electronic communications without the consent of the user. This right will be exercised when there is believed to be a legitimate business reason to do so including, but not limited to those listed below and with the authority of the Director/SIRO/Caldicott Guardian within the organisation.

Details of email systems should be reviewed within the NHS England NHSMail policies.

Email systems should be treated like a shared filing system ie with the expectation that communications sent or received may be made available for review by any authorised employee for purposes related to the organisations business.

Email may constitute “personal records” and be subject to the provisions of the Data Protection Act and Access to Health Records Act. The data subject has the right to access any such records.

Any user who sends or receives communications using non-standard encryption devices to restrict or inhibit access must provide access to such encrypted communications when requested to do so by HBL ICT’s Managing Director or Associate Director of Digital Solutions

3.6 Monitoring Communications

To the extent permitted by law, all electronic communications and their content will be monitored for purposes of:

- Maintaining the integrity and effective operation of systems managed or supported by the organisation
- Ensuring compliance with the organisations policies and procedures and compliance with legislation and statute law

The organisation retains the right to access, review, copy and delete any material created, stored or transported on its systems. This includes but is not limited to messages sent, received or stored on the email system and any material accessed or downloaded from the internet.

Volumes of electronic communications will be monitored routinely including the source, destination and subject of the communication

3.6.1 Inspection and Disclosure of Communications

The organisation reserves the right to inspect and disclose the contents of electronic communications:

- To discharge legal obligations and legal processes and any other obligations to employees, clients, patients, customers and any third parties
- To locate substantive information required for the organisations business that is not readily available by other means
- To safeguard assets and to ensure they are used in an appropriate manner
- In the course of an investigation into alleged misconduct

3.6.2 Special Procedures for Monitoring and Disclosure

Prior approval must be obtained from the appropriate Director/SIRO/Caldicott Guardian to gain access to the contents of electronic data stores and disclose information gained from such access.

3.7 Guidelines for IT Equipment Use

3.7.1 Physical Protection

- Users **shall** not eat or drink in the vicinity of any IT equipment within IT areas e.g. Datacentres, Communications Rooms
- Users should not eat or drink in the vicinity of any IT equipment e.g. laptops.
- Users **shall** not expose any IT equipment to magnetic fields which may compromise or prevent normal operation.
- Users **shall** not expose any IT equipment to external stress, sudden impacts, excessive force or humidity.
- Only authorised IT support personnel **shall** be allowed to open NHS IT equipment and equipment cabinets.
    - If left unattended in semi-controlled areas such as conference centres or customer offices, laptops **shall** be locked to a fixed point using a physical lock available from IT support.

- Portable equipment **shall** never be left unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure.
- Portable equipment **shall** be physically locked down or locked away when left in the office overnight.
- Portable equipment **shall** never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures.
- Portable equipment **shall** not be checked in as hold luggage when travelling, but treated as hand or cabin luggage at all times.

3.7.2 General Use

- Users **shall** lock their terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method) when left unattended, even for a short period.
  - Users **shall** not install unapproved or privately owned software on NHS IT equipment.
  - Only authorised Organisation IT personnel **shall** be allowed to reconfigure or change system settings on the IT equipment.
  - Laptops and mobile devices **shall**:
    - Only be used by the NHS or third party employee that has signed and taken personal responsibility for the laptop.
    - Have the corporate standard encryption software installed, rendering the information on the laptop inaccessible if the laptop is stolen or lost.
    - Have the corporate standard anti-virus, anti-spyware and personal firewall software installed.
    - Have the corporate standard remote access installed.
    - If configured according to the specifications above the laptop/mobile device may be connected to wired or wireless access points.
    - NHS laptops shall never be (via cable or wireless) directly connected to other non-NHS IT equipment or systems.
  - Users **shall** not use privately owned storage devices or storage devices owned by third parties for transfers of NHS data.
  - Any device lost or stolen **shall** be reported immediately and relevant incident process initiated

4 Internet Acceptable Use

- Information found on the Internet is subject to minimal regulation and as such must be treated as being of questionable quality. You **should** not base any business-critical decisions on information from the Internet that has not been independently verified.
- Internet access via the NHS infrastructure is mainly provided for business purposes. For the purpose of simplifying everyday tasks, limited private use **may** be accepted. Such use includes access to web banking, public web services and phone web directories.
- Excessive personal use of the Internet during working hours **shall** not be tolerated and **may** lead to disciplinary action.
- Users **shall** not use Internet-based file sharing applications, unless explicitly approved and provided as a service.
- Users **shall** not upload and download private data (e.g. private pictures) to and from the Internet.
- Users **shall** not download copyrighted material such as software, text, images, music and video from the Internet.
- Users **shall** not use NHS systems or Internet access for personal advantages such as business financial transactions or private business activities.
- Users **shall** not use their organisation's identity for private purposes such as on social media, discussion forums.

4.1 Restrictions on Internet Sites

Restrictions will be placed on access to any internet site that could be regarded as a threat to services, systems and resources, that interferes with the use of the network or other services or to any site that is considered inappropriate. This will include (but is not limited to)

- Sites that attempt to propagate malicious code or any other threat
- Sites containing information that is inappropriate, offensive or unlawful (e.g. pornography, racial bias, gambling and games)
- Downloads or data transfers that threaten or interfere with network or other resources (such as executable files and media streaming)
- Sites that provide "cloud based" storage functionality (e.g. huddle, SkyDrive, iCloud, Dropbox) except where explicitly approved.

Variations to this policy (e.g. where teams require access for work purposes) must be authorized by the relevant SIRO, Caldicott Guardian or DPO and made to HBL ICTs Associate Director of Digital Solutions and approved by HBL ICT Managing

Director or another Associate Director and, should the assessed level of risk warrant it, the Stakeholder Board before being introduced.

Restrictions may be changed or introduced without notice or consultation to preserve the confidentiality, integrity and availability of critical network resources

5 NHS Email Acceptable Use

- Email services within the NHS are provided for business purposes. Limited private use for the purpose of simplifying everyday tasks **may** be accepted but private emails **should** be distributed via web based email services.
- Users **shall** not use external, web-based e-mail services (e.g. hotmail.com) for business communications and purposes.
- Private emails **should** be stored in a separate folder named 'Private e-mail box'. If retrieval of business emails is required (due to sick leave etc.) this folder will not be subject to inspection).
- Private emails **should** be deleted as soon as possible in order to limit storage requirements for non-business information.
- Users **shall** not broadcast personal messages, advertisements or other non-business related information via NHS e-mail systems.
- Users **shall** not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene.
- Users **shall** not distribute statements of a political or religious nature, or other information of a personal nature, unless specifically authorised to do so for business purposes.
- Engaging in any illegal activities via e-mail is prohibited. Discovery of such material **shall**, if deemed as being of a criminal nature, be handed over to the police.
- Information and guidance on sending PCD by Email is available on the NHS Digital NHSMail website

6 Disciplinary Action

Breach of any aspect of this policy will be subject to disciplinary action in line with the organisation's disciplinary policies. Serious breaches will be regarded as gross misconduct and may result in dismissal.

Appendix A. Comment Form

As part of HBL ICT Services Department continuous improvement regime, would you please complete this form. Any comments or feedback on this document should be addressed to the Owner. Please provide your name and contact details in case clarification is required.

Name Click here to enter text.

Address Click here to enter text.

Click here to enter text.

Phone Click here to enter text.

Email Click here to enter text.

Please return to:

HBL ICT Services

Charter House

Welwyn Garden City

Hertfordshire, AL8 6JL

Please confirm the document you want to give response to as:

HBL ICT Policy/Procedure: Click here to enter text.

Please rate the document using the topics and criteria indicated below:

	Very Good	Good	Average	Fair	Poor
Format and Layout	☐	☐	☐	☐	☐
Accuracy	☐	☐	☐	☐	☐
Clarity	☐	☐	☐	☐	☐
Illustrations (tables, figures etc.)	☐	☐	☐	☐	☐

When using the document, what were you looking for?

Click here to enter text.

How could the document be improved?

Click here to enter text.

How often do you use the document?

Click here to enter text.

If you have additional comments, please include them below:

Click here to enter text.

Thank you for your time.