GIG CYMRU NHS WALES | Addysg a Gwella Iechyd Cymru (AaGIC) Health Education and Improvement Wales (HEIW)

IT ACCEPTABLE USE POLICY (AUP)

Executive Sponsor & Function:

Director of Workforce and Organisational Development

Document Author:

Chris Payne

Ricky Hartland

Approved by:

HEIW Executive Team

Approval Date:

11th November 2020

Date of Equality Impact Assessment:

TBD

Equality Impact Assessment Outcome: This policy has been screened for relevance to equality. No potential negative impact has been identified so a full equality impact assessment is not required.

Review Date:

November 2023

Version: v1.0

Table of Contents

1. Introduction

This IT Acceptable Use Policy stipulates the restrictions and practices Health Education and Improvement Wales (HEIW) employees using HEIW IT equipment and resources must agree to as a requirement for accessing and using HEIW facilities, networks, services, and systems.

The intention of this policy is not to enforce restrictions which are opposite to HEIW's promotion of an open, transparent and healthy culture. HEIW is committed to the acceptable use of IT to support appropriate and effective service delivery.

The use of IT equipment, networks, services and systems is central to the day-to-day operations of HEIW. There is a requirement that authorised employees will use these resources correctly and responsibly.

Breach of this IT Acceptable Use Policy may lead to the removal of user access and disciplinary action where applicable.

2. Scope

This policy applies to all relevant parties who have access to or use of HEIW networks, services, systems, information and equipment belonging to or under the control of HEIW, and particularly:

- HEIW IT equipment (e.g. desktop computers, laptops, printers, file shares, servers, web services, mobile devices);
- HEIW permanent and temporary employees;
- Contractors;
- Third Parties;
- Any other parties using HEIW resources.

3. Policy Objectives

The objectives of this IT Acceptable Use Policy comprise of:

- Defining acceptable and unacceptable use of IT equipment, services, systems and networks.
- Increasing employee awareness and publishing good practice.
- Promoting an open, transparent and healthy culture.
- Ensuring the effective use of HEIW resources.
- Avoiding potential liabilities arising from misuse.

4. Definitions

IT Equipment refers to (this list is not exhaustive): desktop computers, laptops, printers, file shares, servers, web services, mobile devices, USB sticks etc.

Proprietary Information refers to: All HEIW information which is considered confidential, sensitive or private including Personally Identifiable Information (PII). PII denotes personal / sensitive personal data / information as defined by the Data Protection Act 2018.

5. Responsibilities

Role	Responsibilities
All HEIW Employees	• Comply with this IT Acceptable Use Policy. • Have a responsibility to use IT equipment appropriately. • Take reasonable steps to ensure no damage is caused to IT equipment. • Must not use IT equipment if they have reason to believe it is dangerous to do so. • Maintain confidentiality and comply with Data Protection & Cyber Security principles and requirements. • Report non-compliance and potential misuse to the local IT team.
Executive Directors	• Responsible for the management of risk within their directorates.
IT Management & Support	• Maintain HEIW IT hardware and software. • Implement administrative, physical and technical security controls. • Investigate policy non-compliance. • Advise Executive Directors and Managers on matters relating to the acceptable use of IT equipment and facilities. • Liaise with NHS Wales Informatics Service (NWIS) on matters requiring resolution.
HEIW Managers	• Ensure employees are made aware of this IT Acceptable Use Policy. • Monitor employee compliance. • Report non-compliance and potential misuse to the local IT team.

6. Policy

6.1. General Use and Conditions

- Information processed, stored and/or transmitted using HEIW IT equipment remains the property of HEIW.

- Employees must ensure that proprietary information is appropriately protected at all times. Personally identifiable information (PII) as defined by the Data Protection Act 2018 must be protected in line with HEIW's Data Protection and Confidentiality Policy.

- Employees must report the loss or theft of IT equipment immediately to the local IT team.

- Employees are responsible for reporting actual or suspected cyber security incidents (e.g. the loss of a laptop) immediately to relevant line management, the local IT team or the Head of Cyber Security.

- Employees must report actual or suspected breaches of this policy to relevant line management and the local IT team.

6.2. Physical Security

- Employees must always wear visible identification (e.g. identification badge).

- Employees must not share an identification badge with other employees or any unauthorised individual.

- Employees must report the loss of theft of an identification badge to the Facilities department or HEIW reception.

- Visitors including contractors and third-party support personnel must always be signed in at reception and accompanied by an authorised HEIW employee.

- Employees are required to report any unescorted visitors, unidentified visitors or any individual not wearing a visible identification badge to the Facilities department, reception or the Head of Cyber Security.

- Doors providing access to and from HEIW facilities and floors must always be secured.

6.3. IT Equipment

- Employees are responsible for the protection of allocated IT equipment.

- Suitable protective mechanisms must be employed to secure IT equipment (e.g. full disk encryption on laptops).

- Employees allocated IT equipment must ensure that appropriate measures are taken to protect IT equipment against damage, loss or theft.

- Employees must ensure that IT equipment under their control is not left unattended in a public place or left in plain sight (e.g. left on a car seat).

- Employees must ensure that unattended IT equipment is protected at all times by:
  - Enabling the password protected screen lock on desktop computers, laptops, mobile devices etc when left unattended.
  - Appropriately terminating active sessions on systems (e.g. servers, networking equipment) once the session is concluded.
  - Appropriately shutting down desktop computers, laptops and other resources when the active session ends or at the end of the working day.
  - Physically securing IT equipment (e.g. laptops) using a cable lock.

- At no time is it permissible for unauthorised individuals (e.g. colleagues, managers, family members) to use HEIW IT equipment.

- Employees must not use allocated IT equipment for the creation and distribution of content or information which is considered defamatory, derogatory, disrespectful, harmful, offensive, profane or in direct violation of the HEIW's Code of Conduct, People Policies, regulations and laws.

- Employees are required to return all IT equipment before leaving their HEIW post.

- Managers must ensure the secure return of IT equipment (e.g. desktop computer, laptop, mobile devices, USB sticks, hardware tokens etc) when an employee leaves a HEIW post and are responsible for informing the local IT team.

- IT equipment must not be re-allocated or moved without appropriate authorisation and consent.

- Employees must report the loss or theft of IT equipment immediately to the local IT team.

- Documents should not be saved and stored locally on desktop computers, laptops, mobile devices etc. These devices are not backed up and as such documents may be irrevocable if the device fails, or is damaged, lost or stolen.

- Employees must not connect unapproved removable media or devices (e.g. CDs, DVDs, USB sticks) to HEIW owned IT equipment.

- Technical measures may be enforced for the secure use of removable media (e.g. CDs, DVDs, USB sticks).

- Inappropriate and unauthorised use of IT equipment will be subject to disciplinary action.

6.4. Access Control

- Revealing or sharing of identification and authentication information (e.g. usernames, ID's, passwords, passphrases, pins, tokens) with unauthorised individuals (e.g. colleagues, managers, family members) is forbidden.

- Passwords should be exclusive and as such, employees must use a unique and separate password for all work-related accounts.

- Employees must not re-use work related passwords for personal accounts.

- Passwords must not be recorded or documented in an unprotected form (e.g. written down on paper).

- Employees must change their password when prompted by the system to do so.

- Employees must enable the password protected screen lock on desktop computers, laptops, mobile devices etc when left unattended.

- Access to networks, services and systems is exercised using the principles of least privilege, need to know, separation of duties and business requirement.

- Managers must ensure that the local IT team are notified of the start date of new employees prior to the actual start date.

- Managers are required to complete the 'new starter request form' to ensure that a user account and appropriate permissions are provisioned for a new employee.

- Managers must ensure that the local IT team is notified when an employee leaves HEIW or changes post. This is of vital importance to ensure that access rights are appropriately revoked for leavers and re-issued for employees who change post.

6.5. Networks and Systems

- The importing of malicious software (malware) onto HEIW networks or systems is forbidden. Examples of malware include: computer viruses, worms, hoaxes, Trojan horses, logic bombs, botnets, spyware, adware and ransomware.

- Employees must not interfere with the operation of anti-malware software installed on IT equipment. This includes and is not limited to:
  - Disabling anti-malware protection;
  - Prohibiting automatic anti-malware software definition updates;
  - Disabling regular anti-malware scanning activities.

- Employee personally owned devices must not be connected to the HEIW network.

- Evading any implemented user identification and authentication mechanisms employed by HEIW is forbidden.

- Conducting network monitoring activities including but not limited to: penetration testing, network scanning and sniffing, port scanning and sniffing, host discovery scanning, vulnerability scanning is expressly prohibited unless expressly authorised by the Information Technology Manager or Head of Cyber Security.

- Disrupting the regular operation of HEIW networks, services or systems for malicious purposes (e.g. network scanning and sniffing, port scanning and sniffing, flood attacks, denial of service etc) is forbidden.

6.6. Software

- Employees must not install unauthorised or unlicensed software on HEIW IT equipment.

- Any employee discovered to be intentionally reproducing software will be subject to the HEIW’s disciplinary policy.

- Employees must not install software which is intended for personal use on HEIW IT equipment.

- Employees must not store personal files or information (e.g. music, videos, images) on HEIW equipment.

- All software programs and applications developed for and / or on behalf of HEIW by employees during the course of their employment will remain the property of the organisation.

- HEIW IT equipment must not be used for the copying, saving or distribution of copyrighted media files (e.g. games, audio CDs, video DVDs).

- All copyrighted information (e.g. images, text, icons, fonts) must only be used with proof of license and/or permission and in accordance with applicable laws and regulations.

6.7. Clear Desk Policy

- Employees must protect HEIW proprietary information from unauthorised access, destruction, disclosure, loss or modification.

- Employees are responsible for securing their designated work area by:
    - Enabling the password protected screen lock on desktop computers, laptops, mobile devices etc when left unattended.
    - Securing paper documents in a locked cabinet.
    - Recovering printed documents from printers.
    - Securing portable / removable media in a locked cabinet.
    - Appropriately terminating active sessions on systems (e.g. servers, networking equipment) once the session is concluded.
    - Appropriately shutting down desktop computers, laptops and other resources when the active session ends or at the end of the working day.

6.8. Email and Internet

- Employees are expected to refer to and comply with the requirements and expected behaviours documented in the All Wales Email Use Policy and All Wales Internet Use Policy.

6.9. Remote Working

- Employees are expected to refer to and comply with the requirements and expected behaviours documented in HEIW's Home and Remote Worker Policy.

6.10. Third Parties

- Third-party access to HEIW networks, services and systems will be administered in conjunction with the NHS Code of Connection.

- Third-party access must be authorised and organised by the Digital department (i.e. IT, Cyber Security).

- Third-party access must comply with the principles of least privilege, need to know and separation of duties.

- Third-party access must be appropriately monitored.

- Audit logs of third-party access to HEIW networks, services and systems should be retained.

- Third-party access must be immediately terminated once the scope of planned and executed work is completed.

6.11. Disposal of IT Equipment

- The local IT team must be notified of any IT equipment which has been identified for disposal.

- All data and software must be appropriately erased from IT equipment prior to disposal, destruction, recycling or re-deployment.

- IT equipment must be securely disposed of in accordance with established operational procedures. IT asset register will be updated to reflect disposal.

6.12. Supporting Policies and Standards

- HEIW's Information Security Policy
- NHS Wales Shared Services Partnership Acceptable Use of IT Procedure
- All Wales Email Use Policy
- All Wales Internet Use Policy
- HEIW's Home and Remote Working Policy
- HEIW's Cyber Incident Response Policy
- National Cyber Security Centre (NCSC) Guidance
- ISO/IEC 27001 / 27002

6.13. Non-compliance

It is the responsibility of all employees to report non-compliance with this policy or the unauthorised use of HEIW IT equipment or facilities.

Contact Information

Contact	Email
Information Technology	HEIW.IT.Team@wales.nhs.uk
Cyber Security	HEIW.CyberSecurity@wales.nhs.uk

Document History

Document Review

Date	Version	Author	Role	Revision Summary
DD/MM/YYYY	**vx.x**	**Name**	**Role: e.g. Head of Cyber Security**	**Description of the revision**
03/07/2020	v0.1	Ricky Hartland	Head of Cyber Security	First draft for comment.
06/07/2020	v0.2	Ricky Hartland	Head of Cyber Security	Document template updated. Minor formatting changes.
06/07/2020	v0.2	Ricky Hartland/Chris Payne	Head of Cyber Security	Updated draft for comment.

Document Approval

Date	Version	Author	Status	Comments / Summary / Approving Body
DD/MM/YYYY	**vx.x**	**Name**	**Draft / Approved**	**Insert Comments / Summary: e.g. Document Approved by HEIW Board**
27/07/2020	v0.2	Chris Payne	Draft Approved	Forwarded for approval from HEIW Executive Team.
11/11/2020	v1.0	HEIW Executive Team	Approved	Document approved by HEIW Executive Team.