Avon and Wiltshire Mental Health Partnership NHS Trust

Acceptable Use Policy (AUP)

Board library reference	Document author	Assured by	Review cycle
P024	Senior Information Governance Manager	IGSG	3 Years

This document is version controlled. The master copy is on Ourspace.

Once printed, this document could become out of date.

Check Ourspace for the latest version.

Contents

1. Policy Statement

This policy forms part of the Trust's Information Governance Management System (IGMS).

Avon and Wiltshire Mental Health Partnership NHS Trust is bound by the provisions of a considerable number of items of legislation and regulation affecting the stewardship of data and information.

Information Governance (IG) ensures the Trust's compliance with applicable legislation, the regulatory framework, Common Law, and mandated best practice. In short, IG exists to ensure the Integrity, Availability, Confidentiality and Accountability of the Trust's operational, patient, staff and management information.

Staff should be aware that IGMS Policies are intended to protect the Trust and staff from adverse outcomes in terms of compliance with the law. Where IGMS policies are breached by staff it may be necessary for managers to consider retraining staff, or following the Trust's Disciplinary Procedures.

This policy is designed to ensure compliance with the:

- The Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990

Together with these NHS Policies:

- The NHS Data Protection and Security Toolkit
- The NHSmail Acceptable Use Policy
- NHS Information Security Management: Code of Practice
- The Caldicott Report 1998
- NHS Confidentiality: Code of Conduct
- NHS Records Management : Code of Practice

Staff should also note that where activity is in breach of the above acts legal penalties, including custodial sentences, can be imposed upon the Trust, its management or directly on the employee for non-compliance with relevant legislation and NHS guidance.

This Policy sets out the baseline standards for the use of Trust Information and Communications Technology systems to ensure the availability of accurate and up to date information in support of the Trust's business objectives. The measures described in this Policy are intended to protect staff, service users and the public from harm arising from the loss, damage, inaccuracy or unavailability of information resources.

Where this policy applies:

- Direct access to AWP IT and communications equipment
- Remote access to AWP IT and communications equipment

2. Scope

This is a Trust-wide Policy and applies to all users of AWP IT systems including employees, locums, contractors, temporary staff, students, service user representatives, volunteers and partner agency staff.

Where a third party has an organisational policy that differs from this Policy, a formal agreement as to which policy statement applies shall be outlined and agreed in an appropriate protocol if necessary. In the absence of such an agreement, this Policy shall be deemed to have precedence.

3. Roles and Responsibilities

3.1 The Chief Executive

is responsible for ensuring the Trust's compliance with applicable legislation and regulation.

3.2 The Director of Finance

is the Trust Senior Information Risk Owner (SIRO) and shall represent any relevant information risk to the Board of Directors. They shall receive specialist advice from the information governance team.

3.3 The Information Governance team

is responsible for this policy, it's implementation and enforcement.

3.4 All users of AWP IT systems

are responsible for ensuring that their use of these systems is conducted in compliance with this policy.

IF IN DOUBT ABOUT ANY OF THE REQUIREMENTS LISTED IN THIS POLICY CONTACT THE INFORMATION GOVERNANCE DEPARTMENT BEFORE YOU ACT

4. Policy Content

4.1 IT Equipment and the AWP Network

The use of Trust IT systems for illegal activity may result in internal disciplinary action and/or the intervention of the Police

Use of the Trust's IT systems is primarily for the purpose of your job role within the Trust and as such, users of the Trust's systems should not have any expectation as to the privacy of their activities whilst using them.

Limited personal use of the Trust IT systems, such as personal emails or producing a document, is accepted so long as such use is kept to an absolute minimum, does not contravene any other conditions of this policy, impact on your work, or the performance of the Trust network. This should not take place during your contracted hours.

You may not use Trust systems to carry out any kind of commercial activity not connected with your contract with the Trust, this including private practice, specialist doctor or similar work.

4.2 Service user and Guest access

Service Users may only access computers specifically provided by the Trust for that purpose.

Under no circumstances should service users, visitors or other guests be give any form of access to the Trusts regular IT systems.

Where available service users, visitors or other guests may use the publically accessible NHS Wi-Fi service.

4.3 You and Your Account

All users are personally accountable for the use of their IT account on Trust systems. You must never share account credentials or smartcards and never allow another user to access systems using your account.

Users must not leave any computer unattended without locking the screen or logging off.

Users should ensure they complete the security questions on the IT Service Desk to enable swift resolution of password resets and set up self-service password reset details for their AWP and NHSmail accounts.

Users should not undertake any activity which poses the threat of introducing viruses or malware to the system. If unsure contact the IT Service Desk for advice before proceeding.

Do not disable or modify any system intended to protect privacy, security or confidentiality of another system, data or person

Users must not add passwords or other security measures to any IT system, application, file or document without first consulting the IT Service Desk

Users must not attempt to remove or bypass the security password protection on any Trust computer or other IT system

4.4 Managing files and data

Users must never attempt to access information, such as medical records, that they do not have a legitimate reason to do so.

All information created during employment with the Trust shall be stored on an appropriate Trust systems – U drive, W & X drives, Ourspace, Media Server, RiO, etc.

Personal documents should not be stored on Trust systems – they may be deleted without prior warning.

Do not attempt to create alternative or new systems for processing Trust data without approval from the IT Department. All Trust data must be contained and processed within approved IT systems.

Bulk data transfers to other organisations should be undertaken by the IT department.

When transferring information outside the Trust you must ensure that this is done securely. If in doubt seek advice from the Information Governance team before proceeding.

Video and audio recordings gathered in the course of Trust business also needs to be stored securely. If you are producing or working with such files you should contact the IT Department to confirm the most appropriate solution to your requirement.

The Trust will not transfer data to any individual leaving the Trust (e.g. no taking U drive information out of the Trust system).

All databases, applications (both locally or hosted online) and any other information processing systems (e.g. web based services) must be approved and registered on the Information Asset Register prior to use. Please contact the IT Department for advice on the correct approval routes.

4.5 Email

Every email is considered public record and therefore discoverable under the Freedom of Information Act 2000 – never attempt to delete, modify or hide any email communication in order to avoid its disclosure.

Emails held within the NHS mail system are not directly retrievable via the AWP IT Department so it is essential that emails containing Trust business are not stored in your email inbox

Never set up auto-forward rules from your mailbox to any location other than sub-folders within that mailbox

Do not send work information to and from personal email addresses to allow you to work at home.

You should avoid using your nhs.net email address for non-work related activity.

Never forward chain letters, advertising, other frivolous material or spam, or distribute rumours or gossip via email and only forward emails if it is relevant to the recipients.

Do not circulate warnings about any virus risk - consult with the IT Service Desk if you receive these

Third party email systems, including all non-NHS webmail facilities, are not generally accessible from the Trust's IT systems and must not be used to transmit or store staff or service user information.

Do not create Outlook .pst files

NHS mail can be viewed from any approved device with internet access but care should be taken to ensure security of the accessible data and that any usage complies with the NHSmail Acceptable Use Policy.

4.6 IT Equipment

All orders for computing/IT resources, including hardware, software, IT services and web-based systems must be raised via the IT Department using an IT work request.

All computers, printers and ancillary IT equipment must only be installed and moved by the IT Department.

When a Trust owned IT device is no longer required, the item must be returned to the IT Department for appropriate disposal.

Any IT equipment or software received from outside parties must be evaluated and approved by the IT department prior to use in the Trust. Staff should check with IT before agreeing to accept any IT equipment not supplied by the Trust's IT Department.

All systems and devices provided by the Trust are subject to the same conditions of use whether they are used remotely (including at home) or on a Trust site.

All network connections must be authorised and installed by the IT Department. Do not connect any device (computer, laptop, printer, tablet, router, modem, wireless network, etc.) to the Trust Network or any part of the Trust system unless the device is owned by the Trust or the connection has been approved and set up by the IT Department. The exception to this is where guest NHS Wi-Fi is provided specifically for use by non-Trust equipment, which is covered by a separate process.

The Trust may disable or remove without warning any device, software or web-based service detected on the Trust's network that has not been authorised and installed by the IT Department.

Do not install any software package on Trust devices. All software, including free/open source software and upgrades to existing packages must be approved, tested and installed by the IT Department

Any unauthorised software found on a Trust device may be deleted or disabled without notice to the user

Users must adhere to the terms and conditions of all licence agreements relating to IT systems including software, equipment, services, documentation and other goods.

4.7 Personal IT equipment

Do not connect non-AWP provided devices to the Trust network through USB ports. This includes (but is not limited to) portable hard drives, memory sticks, memory cards, cameras, mobile phones, iPods, tablets, media players, webcams, keyboards, mice, gamepads. This includes connecting any device for the purpose of charging it.

Privately owned computers or other computing devices (including desktop PCs, laptop computers, tablet PCs, Smartphones, iPads, etc.) may only be used to access Trust systems via the Citrix/SecurEnvoy access route.

Never use your own equipment to create or work on documents unless you are connected to the Trust's systems via Citrix/SecurEnvoy .

Where AWP provided Wi-Fi is available, it's usage by staff is still bound by this policy.

NHSmail may be accessed directly form a personal device provided the device is on the approved list and the required security settings are implemented.

4.8 Partner organisation owned IT equipment (e.g. other NHS Trusts, GPs, Charities or Councils)

Unless agreed otherwise with the partner organisation all access to AWP systems should be via the Trust's Citrix/SecurEnvoy system.

When accessing AWP systems from a partner organisation's device, do not store any information locally on the device or on the host organisation's network unless this has been specifically agreed with the Information Governance team and a suitable Information Sharing Agreement is in place.

When using non-AWP devices at a partner organisation you will also be bound by their policies.

4.9 Internet Access, Social Networking and the Cloud

Access to the Internet using Trust systems is provided and funded for business purposes. Non work-related Internet use consumes capacity on the Trust network and the wider NHS network and may impact business systems such as RiO. As such. any personal usage of the internet via Trust devices (PC, laptop, tablet or mobile phone) should be kept to no more than 20 minutes a day and then only during formal break periods.

Personal internet usage must not exceed 1GB of data per month.

Do not stream media (e.g. TV, radio, films, music videos, YouTube, sports, news) for personal purposes or recreational activity with service users

Do not download or upload music, screensavers, audio, video, desktop wallpapers or any other files for non-work related purposes.

Storage of Trust information via Cloud services e.g. Dropbox, Microsoft One Drive, Google Drive or other providers of "cloud storage services" is not permitted without express consent from the Trust's Information Governance team.

Internet-based applications (Cloud computing) are not generally available across Trust systems i.e. Dropbox, Google Docs, Huddle, Surveys tools and other file storage. Exceptions are agreed on a case by case basis and must have strong business need. Please contact the Information Governance team if you need access.

If social media is part of your role then you must be mindful of the risks of posting Trust information on the internet – refer to the AWP Social Media Policy.

Copyright and usage right law must be complied with at all times. Where images, audio or video content from the internet is used you are required to ensure you can provide confirmation of appropriate usage rights on request.

Online (web based) conferencing is accessible from Trust systems however this need to be set up on a user by user basis. Please contact the IT Service Desk if you require access.

5. Monitoring / Investigations / Incidents and Actions

Monitoring of Trust systems, including all internet usage, happens on a routine basis to ensure compliance with this policy. Monitoring can include unannounced remote viewing/recording of desktop sessions as well as proactive activities designed to identify and respond to potential issues before an incident occurs.

Any suspected breaches of this policy will be managed using the Trust's adverse incident reporting procedures.

Activities that breach this policy, other Trust policies, are a threat to the safety of Trust systems or where personal activity impacts Trust systems or uses excessive amounts of resources may be intercepted and/or prevented as they happen. This may include terminating current activity, disabling of accounts or applying restrictions in usage until the use of your account has been investigated.

Potential breaches will receive a provisional assessment of the activity which may then be followed by a formal investigation in line with the Trust's disciplinary or performance management policies.

The IT Department may use tools and technology to identify breaches and capture potential evidence and record any usage without the user's knowledge or consent. This may include accessing password-protected documents or encrypted web sessions.

A copy of every document stored and audit trails of usage on Trust systems will be archived, and these archives may be used for the investigation of unlawful acts. This may include forensic analysis of any IT systems and system use.

Line Managers are responsible for monitoring that the requirements of this policy have been met by their staff and they are able to request audits from the information governance team to confirm this.

Any issues arising from auditing this policy will be added to the directorate risk register and lead to the creation of an action plan, the implementation of which will be monitored by the Information Governance Steering Group.

Any issues arising from the audit and monitoring of this policy that will aid and inform wider learning will be communicated via the Trust's programme of thematic reviews.

6. Staff Training

Users must ensure they are up to date with all mandatory Information Governance training as well as any mandatory training concerning the use of specific IT systems (e.g. RiO training).

Individual Line Managers are responsible for ensuring their staff are aware and adhere to this policy.

7. Document Lifecycle Control

This policy document forms part of a formal Trust record, and is to be managed in accordance with the Trust's records management policies and retention and disposal schedules.

The Board Policy Document Library on OurSpace is the only recognised repository for master versions of policy documents. Copies of this document are not considered controlled.

8. References

A full list of the applicable legislation referenced in the compilation of this policy can be viewed in the NHS Information Governance Guidance on Legal and Professional Obligations

Version History

Version	Date	Revision description	Editor	Status
1.0	01/07/2006	Trust Acceptable Use Policy	Information Governance Manager	Approved
1.1	18/6/2009	Administrative Changes	Information Governance Manager	Approved
1.2	12/08/2009	Reformatted and Reviewed	Information Governance Manager	Draft
1.3	03/11/2009	Standardisation of Archiving of Master Documents	Information Governance Manager	Draft
2.0	01/12/2009	Approved by Quality and Healthcare Governance Committee	Information Governance Manager	Approved
2.1	25/01/2010	Administrative changes	Information Governance Manager	Approved
2.2	12/11/2010	Administrative Changes	IT Security Specialist	Draft
2.3	17/12/2010	Administrative changes	Information Governance Manager	Draft
3.0	21/01/2011	Reviewed by information Governance Management Group	Executive Director of Finance & Commerce	Approved
3.1	03/06/2011	Review	IT Security Specialist	Draft
4.00	08/09/2011	Approved by information Governance Management Group	Information Governance Manager	Approved
5.00	23/02/2012	Administrative changes and reformatted into Trust Standard Template	IT Security Specialist and Information Governance Manager	Approved
6.00	03/07/2014	Rewritten in line with changes within the Trust and changes in technology	ISTAM & IT Security Specialist	Draft
6.1	24/08/2015	Update guidance on personal internet usage	ISTAM	Approved
7.0	15/01/2019	Review and Update	SIGM	Approved