CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL
INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

NHS Wales Microsoft 365 Acceptable Use Policy for Primary Care Service Providers

Author: IG Support for Primary Care, DHCW
Approved by: Darren Lloyd,
Associate Director of Information Governance and Patient Safety, DHCW
Version: Final V3
Date: September 2023
Review date: September 2025

Ty Glan-yr-Afan
21 Heal Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD
21 Cowbridge Road East, Cardiff CF11 9AD
Ffon/Tel: 02920 500500
www.cymru.nhs.uk/gwybodeg
www.wales.nhs.uk/informatics

Document history

Revision history

Date	Version	Author	Revision Summary
25/06/2020	D0.1	Francesca Harries	Initial draft
29/06/2020	D0.2	Jeannette Short	Updates
9/07/2020	D0.3	Jeannette Short	Updates in conjunction with Carl Walters
14/07/2020	D0.4	Jeannette Short	Feedback from Ian Cox
2/08/2020	D0.5	Jeannette Short	Further updates
21/08/2020	D0.6	Jeannette Short	Feedback/updates from Carl Walters and Darren Lloyd
08/09/2020	D0.7	Jeannette Short	Further updates
17/09/2020	Final Draft D0.8	Jeannette Short	Further updates
21/09/2020	Final V1	Jeannette Short	
13/09/2021	Draft V1.1	Sarah Muirhead	'General Medical Practices' updated to 'Primary Care Service Providers' 'Practice' to 'Organisation' 'NWIS' updated to 'DHCW'
21/04/2022	Draft V1.2	Jeannette Short	Further Updates
22/04/2022	Draft V1.3	Francesca Harries	Further Updates
27/04/2022	Final V2	Francesca Harries	
27/09/2023	Final V3	Francesca Harries	Full review and updates including additional Primary Care Service Providers.

Reviewers

This document requires reviewing by the following individuals

Date	Version	Reviewer Name	Reviewer Title
09/07/2020	D0.3	Ian Cox	Head of Client Services, DHCW
21/08/2020	D0.5	Carl Walters	Principle Project Manager, Client Services, DHCW
21/08/2020	D0.5	Darren Lloyd	Head of Information Governance, DHCW
26/04/2022	Draft V1.3	Darren Lloyd	Associate Director of Information Governance and Patient Safety, DHCW
27/09/2023	V3	Cora Suckley	DPO Service Manager

Authorisation

Signing of this document indicates acceptance of its contents.

Author's Name:	Francesca Harries		
Role:	Deputy DPO Service Manger		
Signature:	27/09/2023 X  Francesca Harries Deputy DPO Service Manager Signed by: Francesca Harries (Fr215649)	**Date:**	27/09/2023

Approver's Name:	Cora Suckley		
Role:	DPO Service Manager		
Signature:	27/09/2023 X  Cora Suckley DPO Service Manager Signed by: Francesca Harries (Fr215649)	**Date:**	27/09/2023

Contents

1. Introduction

NHS Wales Microsoft 365 combines the familiar Microsoft Office applications; Word, Excel, and Outlook (Email) with powerful cloud services, such as OneDrive, SharePoint and Teams, enabling easier communication and collaboration.

The service enhances the existing NHS Wales Email Service by enabling Primary Care Service Providers with access to Outlook and the NHS Wales Global Address List via web browser.

Over time all Primary Care Service providers will be able to access applications within NHS Wales Microsoft 365; allowing them to use a minimum of audio/video conferencing, share desktops, instant message, and share and save files.

For the purpose of this policy 'Primary Care Service Providers', referred to in this policy as the 'organisation' will include General Medical Practices, Prison Health Care Services, Community Pharmacies and Optometrists commissioned to provide primary care services on behalf of NHS Wales.

2. Purpose

This Acceptable Use Policy (AUP) is maintained by Digital Health and Care Wales (DHCW) and sets out the responsibilities of all users, detailed in the scope of this policy, when accessing the NHS Wales Microsoft 365 platform. It determines the acceptable use of the platform and provides assurance that the facilities are being used appropriately to assist in delivery of services.

User responsibilities include but are not restricted to, ensuring that:

- The confidentiality, integrity, availability and suitability of information within the NHS Wales Microsoft 365 platform is maintained by ensuring its use is governed appropriately;
- All individuals as referenced within the scope of this policy are aware of their obligations.

3. Scope and Application

This AUP applies to all staff (users) working for the Primary Care Service providers who have been granted access to the NHS Wales Microsoft 365 platform. It sets out the principles which must be adhered to by all in the use of the NHS Wales Microsoft 365 platform.

The term 'staff' includes all health professionals, partners, employees, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of the organisation.

This policy applies to all staff making use of their NHS Wales Microsoft 365 account via the NHS Wales network infrastructure to access Microsoft 365 applications by any means, regardless of the location from which this is accessed, and the type of equipment used, for example, NHS Wales owned equipment, devices owned by the organisation or personal devices such as mobiles, tablets and laptops operated under a Bring Your Own Device policy.

The organisation should have separate policies, procedures and guides in place for staff use of email, internet services, communication systems, information security, and information governance, which should be read in conjunction with this AUP.

Dependant on the organisation, staff may not have access to all applications set out within this AUP.

4. Roles and Responsibilities

Senior Responsible Person

The person holding the most senior role within the organisation is responsible for ensuring the highest level of organisational commitment to this policy and the availability of resources to support its implementation and any associated legal requirements. Specific responsibilities may be delegated to the representative Data Protection Officer and/or other individuals who have responsibility for information governance within the organisation.

The Senior Responsible Person will take responsibility for the implementation of this AUP within the organisation. They must ensure that all staff are aware of this policy and understand their responsibilities in complying with the policy requirements.

Users

The policy sets out the obligations of users when using the NHS Wales Microsoft 365 applications. These responsibilities include, but are not restricted to, ensuring that:

- Organisational computer systems/devices are not put at risk;
- Users understand their responsibilities and what constitutes abuse of the service;
- Users understand how the NHS Wales Microsoft 365 platform complies with data protection legislation by reading the privacy information.

Owners and Administrators

Microsoft 365 Teams require Owners and Administrators who have overall responsibility for managing a 'Team'. These owners are ultimately responsible for the content of the Team and its lifecycle management. Responsibilities of the owner include:

- Reading, understanding and adhering to this AUP;
- Ensuring data is stored in compliance with the local Records Management Policy and Information Security Policy;
- Ensuring data is managed in line with the compliance and retention policies;
- For managing access to the Team - who has read access and who has edit rights;
- Configuring the Team to meet user requirements;
- Managing permissions for the Team(s);
- Troubleshooting any end-user issues with the Team(s);
- Ensure that the Team content is properly maintained over time and properly archived when the Team has reached the end of its useful life;
- Ensure that the Team always has an active Owner and a backup (before a Team Owner leaves, they must ensure that a new Team Owner is appointed).

Further guidance on Microsoft Team Permissions is available here.

5. Principles of Use

Staff must familiarise themselves with the AUP content and ensure the policy requirements are implemented and followed within their own work area.

All users of NHS Wales Microsoft 365 must complete mandatory Information Governance refresher training at least every two years as appropriate to their organisation.

NHS Wales Microsoft 365 should only be used for approved business and administration purposes, although some limited personal use may be permitted, unless explicitly prohibited by local policy or line management. NHS Wales Microsoft 365 should not be used for non-publicly funded business or for marketing or commercial gain. It has been provided to aid the provision of healthcare and this should be the main use of the service.

Users should ensure they handle and store patient, staff and corporate information in accordance with their classification requirements. For example, personal identifiable information for patients and staff, special categories of information for patients and staff as set out in the UK General Data Protection Regulation and Data Protection Act 2018, and commercially sensitive information or corporate records deemed accessible under the Freedom of Information Act.

Breaches of the policy must be reported via local incident reporting processes and dealt with in line with the relevant human resources policies as appropriate.

Users must treat passwords and/or other access credentials as confidential and protect them appropriately. They must:

- never share their credentials with anyone;
- not store or transmit passwords and other credentials in clear text across any network;
- not write down passwords and leave them on open view;
- not use a single password for more than one account;
- protect the viewing of their password from others when entering the password;
- change their password as soon as they suspect a compromise and raise a security incident with either the DHCW Service Desk or their Line Manager.

When accessing the NHS Wales Microsoft 365 platform, staff must:

- notify their manager immediately if they receive any inappropriate material via any of the Microsoft 365 applications;
- comply with copyright law and all applicable licences, which may apply to software, files, graphics, documents, messages and other material they wish to upload, download or copy;
- not access, store or provide links to inappropriate non-business-related websites, or other resources;
- not display, store, make available or send material, that is illegal, dissimilatory, harassing, obscene, pornographic, libellous, defamatory, breaches any obligations of confidentiality or is otherwise deemed by NHS Wales to be inappropriate in the workplace;

- not illegally copy material protected under copyright law or make material available to others for copying.

NHS Wales Microsoft 365 provides digital communication services such as Email, SharePoint and Teams. To use these services, staff must comply with relevant NHS Wales policies, including:

All Wales Information Governance Policy for Primary Care Service Providers and All Wales Information Security Policy for Primary Care Service Providers.

5.1. NHS Wales Microsoft 365 Applications

Access to the following applications are subject to the service provider and dependant on the requirements of the organisation. Not all applications may be applicable.

5.1.1. Outlook (Email)

Use of Outlook (Email) is governed by the NHS Wales Email Use Policy for Primary Care Service Providers. Users must read the policy in conjunction with this AUP.

5.1.2. Microsoft Teams

Microsoft Teams is a chat and collaboration platform workspace in Microsoft 365, designed to simplify group working. As well as chat-based communications, Teams' integration with other Microsoft services allows users access to shared files, calendars, collaborative editing, and easy switching between voice, video and text chat.

The Teams application is essentially a hub for group chat rooms, which are called channels. Channels also include document libraries which reside on a SharePoint site tied to Microsoft Teams. The Teams application is set up by sending a request to the DHCW Service Desk.

See Section 4 – Roles and Responsibilities for guidance on who and how to set up Teams and Channels.

The general (i.e. non-clinical) use of Teams and its functionalities are provided for the purpose of conducting the business of the Organisation and to assist staff in the performance of their duties. Use is encouraged where it is consistent with the work being undertaken and with the goals and objectives of the Organisation.

Incidental and occasional personal use of Teams is permitted subject to approval of the staff member's line manager, on the understanding that it is legal; it will not impact upon the organisation's business or service provision and it complies with this and any other relevant local policies.

If personal use access is granted, the account holder will be held responsible for any activity undertaken using Teams and its facilities, including information connected to that account, whether carried out by themselves or not.

For the purpose of this AUP, 'Personal Use' of Teams consists of:

- Personal Business Use - Where the use relates to an individual's employment within the organisation or to membership of a Trade Union;
- Personal Private Use - Where the use relates to non-excessive internal colleague communications. If staff are in any doubt what is deemed as acceptable use or non-excessive, they should consult their

line manager or head of service as appropriate. DHCW and the organisation reserve the right to curtail a user's access to the NHS Wales Microsoft 365 platform to safeguard patients, visitors, staff or others and preserve the organisation's reputation and the integrity of its systems.

5.1.3.1. Chat (instant messaging)

Staff must always be aware of the message content when using the chat functionality for work or non-work-related conversations.

The use of chat is considered secure for the transfer of personal identifiable information and business sensitive information. However, users must be vigilant in ensuring all instant messages are sent to the correct recipient. The NHS Wales email address book is linked to Microsoft 365 therefore staff can be identified through this function. Consideration must be given to who will be able to access this information and ensure that it is only shared with other users/individuals on a need-to-know basis. Users must be confident of the privacy settings set to that particular Call, Chat, Team or Channel prior to processing any personal identifiable information.

As well as general awareness of confidentiality and sensitivity of information and use of potentially identifiable information, staff must not:

- Communicate or disclose confidential or sensitive information unless appropriate security measures are in place and it is deemed necessary;
- Communicate any information which in the organisations view could be regarded as offensive or inappropriate. This includes that which can be reasonably deemed to be undesirable, defamatory, abusive, hateful, racist, discriminatory, indecent, obscene, pornographic, unlawful or involves violence, bullying or harassment;
- Communicate or disclose material that is intended to (or in the organisation's view, is likely to) distress, annoy or intimidate another user/individual or is contrary to the organisation's Dignity at Work Policy;
- Send or save information which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist or otherwise illegal material.

Users must be mindful that information disclosed within the Chat application may be subject to access for information requests; see Section 8 - Access to Information Requests for further information.

5.1.3.2. Real time presence

Presence facilities on Teams exist to assist staff to immediately know what staff are online and available to assist with work related matters.

The use of presence facilities is intended to support the organisation's legitimate business requirements and users are encouraged to use this facility for business purposes when it is the most appropriate means of communication.

Users are responsible for all information shared through their own presence status (whether automatically or manually updated) in line with this AUP, including sharing of appropriate content with justified recipients.

5.1.3.3. Screen Sharing

The use of Teams includes the ability to share the desktop application with others and meeting participants.

Authorised users of the platform must ensure that sharing of the desktop or application is appropriate and fits the purpose of the functionality for the work being carried out at that time.

This includes appropriate sharing with other conference participants and guidance set out in this AUP, which includes respecting confidentiality, justified use and appropriate access.

5.1.3.4. Recording a meeting or call

Teams has the capacity to capture audio, video and screen sharing activity, providing Microsoft Stream is enabled. The recording happens in the cloud and is saved to Microsoft Stream.

If users intend to record calls or meetings in any of these formats, they must inform the participants that they will be recorded and obtain all participants permission prior to starting the recording. Any decisions on consent of recording meetings must be respected and all users should be aware that withdrawal of consent can be given at any time.

Consideration should be given to the retention and disposal periods for recordings, with organisational policies being referenced as appropriate. See Section 9 for further details on retention of recordings.

5.1.3.5. Working with third party users

Microsoft Teams allows users of the NHS Wales Microsoft 365 platform to invite third parties (users in other organisations, patients, etc.) to join Microsoft Teams meetings (2-way or multi-party). If the third-party user has the Microsoft Teams app installed on their device, then this can be used. If not, Microsoft Teams runs in a web browser.

All users of the platform that choose to include a third-party to participate using this method must consider the appropriateness of using such functionality, and consider what information is shared with the invited participants.

In some cases, it will be possible for the participants to download any content which is uploaded to the call/conference (files, etc). As such, users need to consider the content of any files which are shared in this way.

5.1.3.6. Use of Teams for clinical purposes

Where it is proposed to use Teams for clinical purposes; for example, video consultations, this must be risk assessed by carrying out a Data Protection Impact Assessment (DPIA). Following the assessment of the risks and any mitigations, the necessary controls should be implemented and authorised by the Caldicott Guardian or other individuals who have responsibility for information governance within the organisation.

In healthcare settings, procedures must be in place to ensure that the platform is used in a manner which is deemed clinically safe. It is also important to note that the chat facility available on Teams should not be used to create a record of the clinical transaction and its conversation.

For further guidance on using Teams for clinical consultations see the IG Guidance on 'Patient Consultations via Video Conferencing'.

5.1.3. OneDrive for Business

OneDrive for Business allows for storing of work-related files and folders. It should not be used for personal files, photographs, media files etc.

When using this application, the following guidelines below must be adhered to:

- Sharing with anonymous individuals is not allowed;
- Periodically review sharing privileges in OneDrive and SharePoint. Remove individuals when they no longer require access to files or folders;
- Share files with specific individuals, never with “everyone” or the “public”;
- Take care when sending links to shared folders, they can often be forwarded to others to whom you did not provide access to;
- Remember that, once a file is shared with someone, and they download it to their device, they can share it with others and any control is lost;
- Staff must report any lost or stolen computer or device that is syncing with OneDrive sync client to the DHCW Service Desk as soon as possible.

All computers and devices that are syncing with OneDrive should be password protected with a strong password, and ideally encrypted to prevent unauthorised data access.

Any documents stored on OneDrive for Business will become inaccessible and unrecoverable 60 days after an employee leaves the organisation or access to Microsoft 365 is removed. It is the responsibility of the ‘Leavers Manager’ to determine what data needs to be retained and then stored in the most appropriate place.

5.1.4. SharePoint Online

SharePoint Online is a cloud-based collaboration platform that integrates with a variety of Microsoft 365 applications and services. Users can easily create, store, collaborate and share content through the use of SharePoint sites and document libraries, access internal sites, documents, and other information from anywhere - at the office or on the go.

When using this application, the following guidelines below must be adhered to:

- Sharing with anonymous individuals is not allowed;
- Periodically review sharing privileges in OneDrive and SharePoint. Remove individuals when they no longer require access to files or folders;
- Share files with specific individuals, never with “everyone” or the “public”;
- Take care when sending links to shared folders, they can often be forwarded to others to whom you did not provide access to;
- Remember that, once a file is shared with someone, and they download it to their device, they can share it with others and any control is lost;

- Staff must report any lost or stolen computer or device that is syncing SharePoint libraries with OneDrive sync client to the DHCW Service Desk as soon as possible.

All computers and devices that are syncing SharePoint libraries should be password protected with a strong password, and ideally encrypted to prevent unauthorised data access.

5.1.4.1. Site Owners Responsibilities

Site owners are ultimately responsible for the content on the site and its lifecycle management. Responsibilities of the site owner include:

- Reading, understanding and adhering to this policy;
- Ensuring data is stored in compliance with the organisation's Records Management Policy and Information Security Policy;
- Ensuring data is managed in line with the compliance and retention policies;
- Managing access to the site, who has read access and who has edit rights;
- Configuring sites to meet user requirements;
- Managing permissions for their site(s);
- Troubleshooting any end-user issues with their site(s);
- Ensure that the site content is properly maintained over time and properly archived when the site has reached the end of its useful life;
- Ensure that the site always has an active Site Owner and a backup (if the current owner is going to leave, they must ensure that a new site owner has been appointed).

5.1.5. Microsoft Forms

Microsoft Forms is a simple to use application that is part of the Microsoft 365 platform which can be used for creating surveys, quizzes and polls. It enables users to quickly create a form, collect responses in real time and view automatic charts to visualise their responses. Users can quickly build a form and forward to responders who can complete it on any browser without having to install separate applications.

When creating or responding to surveys, quizzes or polls in Microsoft Forms users are accepting the following. Staff:

- are responsible for the content and integrity of your survey data and must ensure that you have all the rights and permissions needed to use that content;
- must protect the privacy and confidentiality of colleagues and/or other corporate information, as required by the Organisation's Information Governance policies;
- must not transmit any viruses, malware, or other types of malicious software, or links to such software, through Microsoft Forms;
- must not use Microsoft Forms to infringe the intellectual property rights of others;
- must not use Microsoft Forms to engage in or promote illegal, abusive or irresponsible behaviour, including - in any way that breaches any applicable national or international law, code or

regulation, including data protection and laws relating to unsolicited commercial electronic messages;

- should only request limited personal data (information that identifies individuals) if it is necessary and only for the purpose of processing. For example, names and contact details of respondents should only be requested if they are needed for a specific purpose;
- when requesting or collecting information about the health of patients or colleagues or other special category information, previously known as sensitive information, such as information about racial or ethnic origin, it should be limited as far as possible and consistent to the requirement and audience to which the form is required;
- surveys, even when they may otherwise contain "de-identified" Personally Identifiable Information, may never be used to collect and store respondents' personal information or usernames and passwords;
- all survey data is the property of the organisation;
- all forms should include a short privacy statement detailing why the information is being collected, who will have access to the information and who it will be shared with, and how long it will be kept for

For security, compliance, and maintenance purposes: only authorised personnel may monitor, and audit surveys, quizzes and polls created and circulated in Microsoft Forms.

5.1.6. Microsoft Stream

Microsoft Stream is an enterprise video service where users can upload, view and share videos across NHS Wales Microsoft 365. Staff are responsible for the permissions for the videos uploaded or recorded through Teams.

Staff must not upload videos that contain:

- any information which in the organisations view could be regarded as offensive or inappropriate. This includes that which can be reasonably deemed to be undesirable, defamatory, abusive, hateful, racist, discriminatory, indecent, obscene, pornographic, unlawful or involves violence, bullying or harassment;
- Communicate or disclose material that is intended to (or in the organisation's view, is likely to) distress, annoy or intimidate another person or is contrary to the organisation's Dignity at Work Policy;
- which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist or otherwise illegal material.

5.1.7. Power Platform

The Microsoft Power Platform should not be used to create medical instruments; It should be used for increasing personal productivity through automation, apps, reports and dashboards.

Power Automate

- Premium licences and features such as custom connectors are not supported;
- Connecting to data outside of the NHS Wales Microsoft 365 service is not supported.

Power Apps

- Premium licences and features such as custom connectors are not supported;
- Personal productivity apps should only be created in the default environment.

6. Inappropriate Communications

Regardless of where accessed, users must not use NHS Wales Microsoft 365 to participate in any activity, to create, transmit or store material that is likely to bring the organisation and/or NHS Wales into disrepute or incur liability on the part of the Organisation and/or NHS Wales. For the avoidance of doubt, subject matter considered inappropriate is detailed in Appendix A.

Some users may need to send and receive potentially offensive material as part of their role. Arrangements must be authorised to facilitate this requirement.

When accessing Microsoft 365, you must notify your line manager immediately if you receive any inappropriate material.

7. Personal Identifiable Information (PII) and Business Sensitive Information

As well as general awareness of confidentiality and sensitivity of information and use of potentially identifiable information, staff must not communicate or disclose confidential or sensitive information unless appropriate security measures and authorisation are in place.

NHS Wales Microsoft 365 allows users to invite third parties (users in other organisations, patients, etc.) to join Microsoft Teams meetings (2-way or multi-party). All users of the platform that choose to include a third party to participate must consider the appropriateness of using such functionality, and consider what information is shared with the invited participants. In some cases, it will be possible for the participants to download any content which is uploaded to the conference (files, etc). As such, users need to consider the content of any files which are shared in this way, paying particular attention to all categories of personal identifiable information and business sensitive information.

It should be noted that the applications within Microsoft 365 are not designed to be a formal store for patient information. However, is recognised that individual healthcare professionals may choose to save patient information (including special category data) to individual and group storage areas, to enable availability for day-to-day use. For example, patient information may be processed via Teams as part of a Multi-Disciplinary Team (MDT) whilst performing their public function. This could include sending files with patient information between users of a Teams channel as part of normal processing.

When creating or responding to surveys, quizzes or polls in Microsoft Forms you are accepting the following:

- You must protect the privacy and confidentiality of colleagues and/or other organisational information, as required by local organisation policies;
- You must not request personal data (information that identifies individuals) unless it is required, and this should be limited in its nature. For example, names and contact details of respondents should only be requested if they are needed for a specific purpose;

- You must not request or collect information about the health of patients or colleagues or other sensitive information, such as information about racial or ethnic origin through Microsoft Forms.

Surveys, even when they may otherwise contain “de-identified” Personally Identifiable Information, may never be used to collect and store respondents’ personal information or usernames and passwords.

If you intend to record Teams video calls or conferences, you must inform the participants that you will be recording and receive all participants permission. You are responsible for the permissions for the videos you upload or record through Teams. Staff should be reminded that any information captured whilst a call or conference is being recorded through Microsoft 365 applications, may be subject to requests for information, see Section 8 for further details.

8. Access to Information

Information held on computers, including those held on Microsoft 365 may be subject to requests for information under relevant legislation and regulation. All staff should be mindful that it may be necessary to conduct a search for information and this may take place with or without the author’s knowledge or consent.

9. Records Management

Users must ensure all business, patient and client information is handled and stored in accordance to the Records Management Code of Practice for Health and Social Care 2022. At the time of writing, the Email and Teams retention policy is set for 7 years. A national programme of work is currently considering further agreement on specific retention periods for the various applications within Microsoft 365; this AUP will be updated to reflect any changes, such as national records management policies are set.

OneDrive for Business may be used to store users work-related files. It should not be used for personal files, photos, media files, etc.

Users must ensure that data on OneDrive for Business is stored in compliance with their organisations Records Management Policy and Information Security Policy.

Any document stored on OneDrive for Business will become inaccessible and unrecoverable **60** days after an employee leaves, it is the responsibility of the employee to determine what data needs to be retained, and then stored in an appropriate place.

10. Training and Awareness

Information Governance is everyone’s responsibility and is mandatory. Staff must undertake appropriate information governance training in line with the requirements of their role.

The organisation workforce should become competent in using NHS Wales Microsoft 365 to the level required of their role in order to be efficient and effective in their day-to-day activities. Training videos have been developed locally to support some of the Microsoft 365 applications and are available on the DHCW Microsoft 365 Centre of Excellence, further guidance can be found through the Help icon within the Teams platform.

11. Monitoring

NHS Wales trusts its workforce; however, it reserves the right to monitor work processes to ensure the effectiveness of the service. This will mean that any personal activities that staff undertake in work may come under scrutiny. Organisations within NHS Wales respect the privacy of its employees and does not want to interfere in their personal lives but monitoring of work processes is a legitimate business interest.

Staff should be reassured that NHS Wales takes a considered approach to monitoring; however, it reserves the right to adopt different monitoring patterns as required. In the main, monitoring is normally conducted where it is suspected that there is a breach of either NHS Wales policy or legislation. Furthermore, on deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

Managers are encouraged to speak to staff of their concerns should any minor issues arise. If breaches are detected an investigation may take place. Where this or another policy is found to have been breached, disciplinary action may be taken.

12. Review

This Acceptable Use Policy will be reviewed every two years or where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Changes in the technology; or
- Changing methodology.

The effectiveness of this policy will be assessed to provide assurance that risks to information and the likelihood and impact of information security incidents are being reduced.

13. Further Support

The DHCW Service Desk can be contacted via the Self Service Portal or by calling 0333 200 8048.

Appendix A - Inappropriate use

For the avoidance of doubt, NHS Wales will generally consider any of the following inappropriate use:

- Knowingly using another person's NHS Wales Microsoft 365 account and its functions, or allowing their Microsoft 365 account to be used by another person;
- Allowing access to NHS Wales internet services by anyone not authorised to access the services, such as by a friend or family member;
- Communicating or disclosing confidential or sensitive information unless appropriate security measures and authorisation are in place;
- Communicating any information which could be regarded as offensive or inappropriate. This includes that which can be reasonably deemed to be undesirable, defamatory, abusive, hateful, racist, sexist, homophobic, transphobic, discriminatory, indecent, obscene, pornographic, unlawful or involves violence, bullying or harassment;
- Communicating or disclosing material that is intended to distress, annoy or intimidate another person or is contrary to the Organisation's Dignity at Work Policy;
- Sending or saving information or images which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist, sexist, homophobic, transphobic or otherwise illegal material;
- Knowingly breaching copyright or Intellectual Property Rights (IPR);
- 'Hacking' into others' accounts or unauthorised areas;
- Deliberately attempting to circumvent security systems protecting the integrity of the NHS Wales network;
- Any purpose that denies service to other users (for example, deliberate or reckless overloading of access links or switching equipment);
- Deliberately disabling or overloading any ICT system or network, or attempting to disable or circumvent any system intended to protect the privacy or security of employees, patients or others;
- Intentionally introducing malicious software such as Viruses, Worms, and Trojans into the NHS Wales network;
- Expressing personal views that may bring the organisation or NHS Wales into disrepute;
- Distributing unsolicited commercial or advertising materials;
- Communicating unsolicited personal views on political, social, or religious matters with the intention of imposing that view on any other person. This does not preclude Trade Union officials from communicating with staff on Trade Union related matters;
- Obtaining or distributing unlicensed or illegal software via the NHS Wales Microsoft 365 platform;
- Installing additional related software, or changing the configuration of existing software without appropriate permission;
- Sending unlicensed or illegal software or data including executable software, such as shareware, public domain and commercial software without correct authorisation;
- Forwarding chain messages or spam (unsolicited messages) within the organisation or to other organisations;
- Sending personal photos or videos.