GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW / STP04 **Version Number:** 1 **Date of next review:** December 2024

OFFICE 365 ACCEPTABLE USE PROCEDURE

Procedure Statement

The Procedure sets out the responsibilities of all users when using Microsoft Office 365 in Public Health Wales to ensure facilities are used appropriately in delivering services.

Procedure Commitment

To set out the principles which must be adhered to by all in the use of Microsoft Office 365 services.

Supporting Procedures and Written Control Documents

Other related documents are:

All Wales Information Governance Policy
All Wales Information Security Policy

Scope

This Procedure applies to all those making use of their Public Health Wales Microsoft Office 365 account via the NHS network infrastructure and / or NHS equipment to access Microsoft Office 365, regardless of the location from which this is accessed and the type of equipment used.

Equality and Health Impact Assessment	An Equality and Health Impact Assessment has been undertaken.
Approved by	Leadership Team
Approval Date	16 December 2021
Review Date	December 2024
Date of Publication:	December 2021
Group with authority to approve supporting procedures	N/A
Accountable Executive Director/Director	Executive Director of Quality, Nursing and Allied Health Professionals
Author	Jonathan Cook, Project Support Officer

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or Corporate Governance.

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**

1. Purpose

This Procedure sets out the responsibilities of all users when using Microsoft Office 365 for Public Health Wales to ensure that those facilities are used appropriately in delivering services. These responsibilities include, but are not restricted to, ensuring that:

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

This policy should be read in conjunction with other relevant organisational procedures.

2. Scope and Application

This Procedure applies to all Public Health Wales staff.

It sets out the principles to be adhered to by all members of staff in the use of Microsoft Office 365 services.

This Procedure applies to all those making use of their Public Health Wales Microsoft Office 365 accounts via the NHS network infrastructure and / or NHS equipment to access Microsoft Office 365, regardless of the location from which this is accessed and the type of equipment used.

NHS Wales has separate policies and guides for staff use of Email and Internet services, Information Security and Governance which should be read in conjunction with this Procedure.

3. Acceptable Use

3.1. General Guiding Principles

Users of Microsoft Office 365 need to have completed the mandatory Cyber Awareness and Information Governance e-learning modules and had security training at induction, or as part of their mandatory training.

- Microsoft Office 365 should only be used for approved business purposes, though some limited personal use may be permitted, unless explicitly prohibited by local policy or line management.
- Microsoft Office 365 applications should not be used to create medical devices[1] without prior engagement of the Executive Director of Quality, Nursing and Allied Health Professionals.
- Ensure you handle and store all Public Health Wales, client information in accordance to their classification requirements.
- You must treat passwords and / or other access credentials as confidential and protect them appropriately, you must:

- Never share your credentials with anyone.
- Not store or transmit passwords and other credentials in clear text across any network.
- Not write down password and leave it in open view.
- Not use a single password for more than one account.
- Protect the viewing of your password from others when entering the password.
- Change your password as soon as you suspect a compromise and raise a security incident with either local IT helpdesk or Security Support or Manager.

When accessing Microsoft Office 365, please ensure that you:

- Notify your manager immediately if you receive any inappropriate material.
- Comply with copyright law and all applicable licences, which may apply to software, files, graphics, documents, messages and other material you wish to upload / to download or copy.

[1] The Medicines and Healthcare products Regulatory Agency defines a medical device as "any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnosis or therapeutic purposes or both and necessary for its proper application, which is intended by the manufacturer to be used for human beings for the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease, diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, investigation, replacement or modification of the anatomy or of a physiological process, or control of conception."
https://www.gov.uk/guidance/medical-devices-how-to-comply-with-the-legal-requirements

- Not access, store or provide links to inappropriate non-business-related websites or other resources. Which display, store, make available or send material which is illegal, discriminatory, harassing, obscene, pornographic, libellous, and defamatory, breaches any obligations of confidentiality or is otherwise deemed by Public Health Wales to be inappropriate in the work place.
- Not illegally copy material protected under copyright law or make material available to others for copying.

3.2. Services Specific to Office 365

Microsoft Office 365 provides digital communication services such as Email, Teams, SharePoint and Yammer, in using these services you agree to:

- Comply with all relevant NHS Wales policies, including;
- Information Security Policy.
- Email Use Policy.

3.2.1. Outlook (Email)

Using Outlook (Email) is governed by the All Wales Email Use Policy, please read this policy and understand its acceptable use guidelines.

3.2.2. Microsoft Teams

General (i.e. non-clinical) use of Teams is provided for the purpose of conducting the organisation's business and to assist staff in the performance of their duties.

The use of Teams is encouraged where it is consistent with the work being undertaken and with the goals and objectives of the organisation.

Where users wish to use Welsh in Teams for either attending or facilitating meetings or contacting individuals and persons the normal provisions under the Welsh Language Standards will apply.

When using Teams it is important to consider the wellbeing of other users. Some good practices being adopted across Public Health Wales consist of not booking meetings during lunchtimes as well as ensuring that meetings have a space between them to enable breaks between consecutive meetings. Please discuss any preferred wellbeing requirements with your colleagues and teams as needed.

Incidental and occasional personal use of Microsoft Teams is permitted providing it will not impact upon the organisation's business or service provision.

The account holder is held accountable for any activity undertaken using Microsoft Teams and its facilities, including information connected to that account, whether carried out by themselves or not.

'Personal Use' of Teams consists of:

- Personal Business Use – Where the use relates to an individual's employment within an NHS organisation;
- Personal Private Use – Where the use relates to non-excessive internal colleague communication. If staff are in any doubt as to what is deemed as acceptable use or non-excessive, they should consult their line manager or head of service. NHS Wales reserves the right to curtail an employee's access to Teams to safeguard patients, visitors, staff or others and preserve the organisation's reputation and the integrity of its systems.

3.2.2.1. Chat (Instant Messaging in Teams)

Staff should be aware at all times of message content when using the chat functionality to enter into work or non-work conversations. Anything within the chat function of Teams is searchable for the purpose of Freedom of Information and Subject Access Requests for personal data. The chat function must not be used when sending messages that contain:

- Any personal identifiable information relating to patients (or people linked to the patients) or staff, without the subject's consent;
- Any personal information relating to patients, or people linked to patients, or staff that might be identifiable from the context or location, without that person's consent;
- Any statements by or on behalf of the organisation that have not been approved by Corporate Communications;
- 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.

- 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 and 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 Respect and Resolution Policy.
- Send or save information which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist or otherwise illegal material.

In a clinical setting, it is also important to note that the Instant Messaging facility available on Teams should only be used for initiating the consultation and should not be used to create a record of the clinical transaction and its conversation.

3.2.2.2. Real Time Presence (in Teams)

Presence facilities on Teams exists to assist staff that work remotely to know if staff are online and available to assist with work related matters.

The use of presence facilities are 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 the acceptable use guidance in the section general guiding principles above, including sharing of appropriate content with justified recipients.

3.2.2.3. Screen Sharing in Teams

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

- Authorised users of the platform need to 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 the general guiding principles which includes respecting confidentiality, justified use and appropriate access.

3.2.2.4. Working with Third Party Users

Microsoft Teams allows NHS Wales users 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 is 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 need to consider the appropriateness of using such functionality and consider what information is shared with the invited participants.

3.2.2.5 Recording in Teams

Before making recordings of meetings in Teams some considerations need to be taken into account.

The first consideration is for any personal data which may be disclosed during the meeting. If an individual is knowingly being discussed, and they can be identified from that recording, the meeting should not be recorded.

The other consideration is that if you are choosing to record the meeting then there must be a robust business reason for taking the recording.

Recordings made in Teams are subject to Freedom of Information Requests and will be made available to the public if requested. Therefore, you must always consider any implications under the Freedom of Information Act 2000 when making recordings in Teams. If a meeting is being recorded, do not say anything which you would not be want to be heard outside of that meeting. All meetings have the potential to disclose personal data. If you make a recording in Teams and it contains the personal information of any individual, please inform the Information Governance team prior to sharing. Please also consider the following when recording in Teams:

- All meeting recordings can be subject to Freedom of Information Requests and might be made public.
- If you intend to record Teams video calls or conferences you must inform the participants that you will be recording.

- You are responsible for the permissions for the videos you upload or record through Teams.
- 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. All users that use this function will need to follow the general guiding principles that includes appropriate use and justification of communication using this function.
- Once you have completed your use of the recording, such as for completing the minutes of a meeting, the recording must be deleted.

3.2.3. OneDrive for Business

- OneDrive for Business should be used to store your work-related files. It should not be used for personal files, photos, media files, etc. It should not be used as/or replace the Public Health Wales Corporate Document Management System (hosted on the Public Health Wales Intranet).
- All of your computers and devices that are syncing with One Drive shall be password protected with a strong password and ideally encrypted to prevent unauthorized data access.
- Any document stored on OneDrive for Business will become inaccessible and unrecoverable 60 days after an employee leaves. It is the responsibility of the leaver's manager to determine what data needs to be kept and then place it in an appropriately accessible place.
- OneDrive for Business allows the sharing of files and folders with others. When sharing files and folders with others the following guidelines must be followed:

- Anonymous sharing is not allowed.
- Periodically review sharing privileges in OneDrive: Remove individuals when they no longer require access to files or folders.
- Share files with specific individuals, never with "everyone" or the "public".
- Be careful sending links to shared folders because they can often be forwarded to others to whom you did not provide access.
- Remember that, once a file is shared with someone, and they download it to their device, they can share it with others.
- You shall report any lost or stolen computer or device that is syncing with OneDrive to Client Services as soon as possible.

3.2.4. SharePoint Online

- SharePoint Online should be used to store your Teams work-related files. It should not be used for personal files, photos, media files, etc. It should not be used as/or replace the Public Health Wales Corporate Document Management System (hosted on the Public Health Wales Intranet).
- SharePoint allows the sharing of files and folders with others. When sharing files and folders with others the following processes must be followed:
    - Anonymous sharing is not allowed.
    - Periodically review sharing privileges in your site: Remove individuals when they no longer require access to files or folders.
    - Share files with specific individuals, never with "everyone" or the "public".
    - Be careful sending links to shared folders because they can often be forwarded to others to whom you did not provide access.
    - Remember that, once a file is shared with someone, and they download it to their device, they can share it with others.
    - You shall report any lost or stolen computer or device that is syncing SharePoint Libraries with the OneDrive sync client to Client Services as soon as possible.

3.2.5. Site Owners Responsibilities

A SharePoint Site Owner is a user with Full Control privileges to the given SharePoint site. 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 Public Health Wales Corporate Document Management Policy and the NHS Wales Information Security Policy.
- Ensuring data is managed in line with 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).

3.2.6. Microsoft Forms

When creating a survey, quiz or poll in Microsoft Forms which will collect personally identifiable information a Data Protection Impact Assessment (DPIA) should be completed. A DPIA is a process designed to help you to identify, analyse and minimise any potential data protection risks. Please contact the Public Health Wales Information Governance team so that they can support and assist you with the completion of a DPIA if one is needed.

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

- You 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.
- You will protect the privacy and confidentiality of colleagues and/or other Public Health Wales information, as required by Public Health Wales Information Governance policies.
- You will not transmit any viruses, malware, or other types of malicious software, or links to such software, through Microsoft Forms.
- You will not use Microsoft Forms to infringe the intellectual property rights of others.
- You will 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.
- You will 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 will not request or collect information about the health of patients or colleagues or other sensitive information, such as information about racial or ethnic origin.

- 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 Public Health Wales.

Microsoft Forms is not intended as a mechanism through which patients are engaged; proposals for patient questionnaires or engagement should be submitted through the normal channels.

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

3.2.7. Microsoft Stream

You are responsible for the permissions for the videos you upload or record through Teams.

You 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, and 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 Respect and Resolution Policy.
- Which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist or otherwise illegal material.
- Any videos which contain the personal information of staff, patients or service users for any reason, without explicit consent.

3.2.8. Power Platform

Microsoft Power Platform is a collective term for the range of apps developed by Microsoft to help with automating and analysing data. These include Power Automate and Power Apps. The platform should not be used to create medical devices[2]; it should be used for increasing personal productivity through automation, apps, reports and dashboards.

3.2.8.1. Power Automate

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

3.2.8.2. Power Apps

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

4. Monitoring and Compliance

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 the employee practices in work may come under scrutiny. NHS Wales's organisations 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's organisations take a considered approach to monitoring, however it reserves the right to adopt different monitoring patterns as required. Monitoring is normally conducted where it is suspected that there is a breach of either 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. For example, all staff have

[2] The Medicines and Healthcare products Regulatory Agency defines a medical device as "any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnosis or therapeutic purposes or both and necessary for its proper application, which is intended by the manufacturer to be used for human beings for the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease, diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, investigation, replacement or modification of the anatomy or of a physiological process, or control of conception."
https://www.gov.uk/guidance/medical-devices-how-to-comply-with-the-legal-requirements

the right to use Welsh to correspond while using Office 365. As is the law under the Welsh Language (in Wales) Measure 2011.

Managers are expected 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 Procedure is found to have been breached, disciplinary procedures will be followed.

Concerns about possible fraud and/or corruption should be reported to the Counter Fraud team.

5. Review

This Procedure will be reviewed every three years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Practice change or change in system/technology; or
- Changing methodology.