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

NHS Wales Email Service, incorporating NHS Wales Office 365 Teams *Lite*

Acceptable Use Policy for Primary Care Service providers

Author: IG Support for Primary Care, NWIS
Approved by: Darren Lloyd, Head of Information Governance, NWIS
Lloyd Hambridge, Welsh Clinical Fellow, Welsh Government
Version: Final V1
Date: September 2020

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
05/08/2020	D0.1	Jeannette Short	Initial development
11/09/2020	D0.2	Jeannette Short	Updates follow initial feedback from CC
21/09/2020	D0.3	Jeannette Short	Updates following feedback from EW
23/09/2020	V1	Jeannette Short	

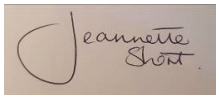
Reviewers

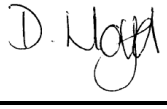
This document requires reviewing by the following individuals

Date	Version	Reviewer Name	Reviewer Title
28/08/2020	D0.1	Claire Chalmers	Project Manager, PCS, NWIS
28/08/2020	D0.1	Emma Williams	Pharmacy Clinical Lead, ICT Programmes, NWIS

Authorisation

Signing of this document indicates acceptance of its contents.

Author's Name:	Jeannette Short
Role:	Primary Care Support and IG Assurance Manager
Signature:	30/10/2020 X  Jeannette Short Primary Care Support and IG Assurance Man... Signed by: Jeannette Short (Je126730)

Approver's Name:	Darren Lloyd
Role:	Head of Information Governance, NWIS
Signature:	30/10/2020 X  Darren Lloyd Head of Information Governance Signed by: Jeannette Short (Je126730)

Approver's Name:	Lloyd Hambridge
Role:	Welsh Clinical Fellow, Welsh Government

Signature:	30/10/2020 X  Lloyd Hambridge Welsh Clinical Fellow Signed by: Jeannette Short (Je126730)

Contents

1. Introduction

This service enhances the existing NHS Wales Email Service by enabling Primary Care Services providers, including Pharmacists, Dentists to access Outlook and benefit from features such as Chat, Video and Voice Calls, (Teams *Lite*) and access to the NHS Wales Global Address List via web browser.

The service enables easier communication and collaboration providing users with access to audio/video conferencing, share desktops, instant message, and share files with; for example, colleagues, patients, carers and support workers that are geographically separated.

2. Purpose

This Acceptable Use Policy (AUP) is maintained by NHS Wales Informatics Service (NWIS) and sets out the responsibilities of all users, detailed in the scope of this policy, when accessing the NHS Wales Office 365 platform. It determines the acceptable use of the platform and provides assurance that the NHS Wales Office 365 facilities are being used appropriately to assist in delivery of services. It ensures all individuals as referenced within the scope of this policy are aware of their obligations.

Staff contact details are made available in the NHS Wales Global Address List to support delivery.

NHS Wales Office 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.

3. Scope and Application

This AUP applies to all staff (users) within the Primary Care Service provider who have been provided access to the NHS Wales Office 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. It sets out the principles which must be adhered to by all in the use of the NHS Wales Office 365 platform.

For the purpose of this policy ‘Primary Care Service providers’, referred to in this policy as ’the Organisation’ will include General Medical Practices, Pharmacies, Dentists and Optometrists commissioned to providing primary care services on behalf of NHS Wales.

This policy applies to all those making use of the NHS Wales Email Service and Teams *Lite* facilities via the NHS Wales network infrastructure, by any means regardless of the location from which accessed and type of equipment used, for example corporate equipment, devices owned by your Organisation or personal devises operated under a Bring Your Own Device scheme (BYOD).

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.

4. Roles and Responsibilities

The Senior Responsible Person 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 will be delegated to the appointed Information Governance Lead or similar as appropriate.

They must ensure that all staff are aware of this policy, understand their responsibilities in complying with the policy requirements.

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

- organisational computer systems/devices and personal devices are not put at risk;
- users understand their responsibilities and what constitutes abuse of the service;
- users understand how the NHS Wales Office 365 platform complies with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) by reading the Privacy Information.

5. NHS Wales Office 365 Applications

5.1. Principles for the use of NHS Wales Office 365

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 Office 365 must complete their respective mandatory Information Governance training least every two years.

NHS Wales Office 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.

Users should ensure they handle and store patient, staff and corporate information in accordance to 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 General Data Protection Regulation and Data Protection Act, 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 policy where 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 password and leave it in 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 NWIS Service Desk or their Line Manger.

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

- notify their manager immediately if they receive any inappropriate material;
- 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;
  - which display, store, make available or send material, which 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 Office 365 provides digital communication services such as Email and Teams Lite. To use these services, staff must comply with relevant NHS Wales policies, including:

- NHS Wales Information Governance Policy;
- NHS Wales Information Security Policy;

Note: these All Wales policies are currently being reviewed to incorporate Primary Care Service providers, in the meantime the principles will apply.

5.2. 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. The NHS Wales Email system is considered a secure method for transferring information, including personal information within NHS Wales, this includes email addresses ending in "wales.nhs.uk". The NHS Wales email address book is available for staff to check the identity of other users on the NHS Wales Email system. Users should still consider the use of encryption for transferring 'special categories' of information, to mitigate against the risk of misdirection, etc.

5.3. Chat (instant messaging) and Calls

Users within Primary Care Services have access to a chat-based voice and video application and text chat/instant messaging application which is designed to simplify group working.

The use of Chat and Calls is considered secure for the transfer of personal 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 Office 365 therefore staff with NHS Wales email addresses 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 Calls or Chats prior to processing any person 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 Organisation's 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;

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

Users must be mindful that information disclosed within the Chat application may be subject to access for information requests; see Section 9 Access to Information for further information

5.3.1. Real time presence

Presence facilities on Teams exist to assist staff that work remotely 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 acceptable use guidance including sharing of appropriate content with justified recipients.

5.3.2. 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 these guiding principles which includes respecting confidentiality, justified use and appropriate access.

5.3.3. Working with third party users

Microsoft Teams allows users of the NHS Wales Office 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 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 these general guiding principles that includes appropriate use and justification of communication using this function.

5.3.4. Recording a Teams Meeting or Call

Teams has the capacity to capture audio, video and screen sharing activity. 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 8 for further details on retention of recordings.

5.3.5. Use of Teams for clinical purposes

Where it is proposed to use Teams for clinical purposes; for example, video consultations with patients, 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 Data Protection Officer. In clinical surroundings procedures must be in place to ensure that the platform is used in a manner which is deemed clinically safe. For further guidance on using Teams for consultations see the IG Guidance on 'Patient Consultations via Video Conferencing'.

6. Inappropriate Communications

Regardless of where accessed, users must not use NHS Wales Office 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 organisations. For the avoidance of doubt, subject matter considered inappropriate is detailed in Appendix B.

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 Office 365, you must notify your 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 Office 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 person identifiable information and business sensitive information.

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 Office 365 applications, may be subject to requests for information, see Section 9 for further details. For further guidance on using Teams for consultations see the IG Guidance on '[Patient Consultations via Video Conferencing]'.

8. Records Management

Users must ensure all business, patient and client information is handled and stored in accordance to their classification requirements. At the time of writing, the NHS Wales email retention policy is set for 7 years, with legal hold enabled. A national programme of work is currently considering further agreement on specific retention periods for the various applications within Office 365; this AUP will be updated to reflect such as policies are set.

It is also important to note that the Chat - instant messaging facility should only be used for initiating the consultation and should not be used to create a record of the clinical transaction and its conversation.

9. Access to Information

Information held on computers, including that held in NHS Wales Office 365, may be subject to requests for information under relevant legislation and regulations; for example, Subject Access Request under data protection

All staff should be mindful that it may be necessary to conduct a search for information within any of the NHS Wales Office 365 applications. Administration tools are available to help find personal information in response to Subject Access Requests (SAR), for example, email, documents, and instant messaging.

Each Primary Care Service provider on the NHS Wales Office 365 tenancy will be a Data Controller and therefore responsible for processing a SAR applicable to their data.

10. Training and Awareness

Governance is everyone's responsibility. Training is mandatory, staff must have appropriate information governance training in line with the requirements of their role.

The Organisation's workforce should become competent in using NHS Wales Office 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 Office 365 applications and are available via the [NWIS website], further guidance can be found through the Help icon within the Teams platform.

11. Monitoring and Compliance

NHS Wales and the Organisation 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. 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 and the Organisation 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 likelihood and impact of information security incidents are being reduced.

13. Further Support

NWIS Service Desk can be contacted via:

- the Self Service Portal https://nwis-service-portal.wales.nhs.uk/Login?ReturnUrl=%2F
- Emailing - primaryare.servicedesk@wales.nhs.uk; or
- Calling 0333 200 8048 or Line Manager.

Appendix A – Points to note

There are a range of points that need to be considered when planning how NHS Wales Email and Office 365 accounts should be used.

- Email is a useful additional communication channel, but if the information being communicated to the Organisation is time sensitive, the Organisation must have procedures in place to ensure these communication channels are checked on a frequent basis;
- Problems can sometimes arise when attachments are sent to the Organisation to view or edit, but the Organisation doesn't have the necessary software on their computer to support this. As there is a risk that unapproved software could interfere with the operation of the Organisation's system or invalidate the Organisation's maintenance contract with their supplier, it is important to check with suppliers before loading software on to the Organisation's computers;
- Many Organisations have strict controls for the websites that can be accessed from the Organisation's computer. In some cases, staff can only access a list of sites that have been pre-approved by a company Head Office. Therefore, when sending emails, it should be considered that any links within these communications may not be accessible;
- Thought should be given to who will have access to the shared mailbox and how will this access be managed. Processes should be put in place to ensure access rights are maintained when there are staff changes;
- Storing records of clinical communications is important for clinical governance reasons. NHS Wales Email is designed to support the transfer of information, not the storage of information. Whilst some information could be copied across to the notes in the patient's record, particular consideration will need to be given to how attached documents are stored (including arrangements for data back-up and appropriate access controls);
- NHS Wales Email is the only NHS Wales approved method for exchanging patient data by email, however this is only if both sender and recipient use NHS Wales Email accounts;
- Appropriate information governance procedures need to be put in place if NHS Wales Email is used to transfer special categories of information. As NHS Wales Email can be accessed anywhere, it is not possible to limit access rights to a particular location, for example from within an Organisation. Also, NHS Wales Email can be linked to a wide range of mobile devices; if this option is used, provision needs to be made for the event that they are stolen or lost, for example a process to activate self-wipe capability.

Appendix B - 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 Office 365 account and its functions, or allowing their Office 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 Office 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.

Appendix C – Glossary of Terms

Term	Definition
Primary Care Service providers	General Medical Practices, Pharmacies, Dental Practices and Optometrists
Senior Responsible Person	**General Medical Practice –** Senior Partner, Caldicott Guardian, Data Protection Officer, Senior Information Risks Officer, Information Governance Lead, Practice Manager, etc **Pharmacies –** Pharmacy Owner, Superintendent, Information Governance Lead, etc **Dental Practice** – Senior Partner, Information Governance Lead, etc **Optometrists** – Senior Partner, Information Governance Lead, etc
Staff	This is not an exhaustive list: all health professionals, partners, employees, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of the Primary Care Service provider.