Ashford and St. Peter's Hospitals
NHS Foundation Trust

Microsoft Office 365 Acceptable Use Policy

Author: Nicki Rayment – Head of Digital Programme Delivery

Executive Lead: Simon Marshall – Director of Finance and Information

Status: Approval date: July 2021

Ratified by: IG Steering Group

Review date: July 2024

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Ratified by
1	July 2021	New policy	IG Steering Group

For more information on the status of this document, please contact:	
Policy Author	Nicki Rayment – Head of Digital Programme Delivery
Department/Directorate	Digital Services
Date of issue	July 2021
Review due	July 2024
Ratified by	Information Governance Steering Group
Audience	All staff

Executive summary

O365 (Office 365) is a suite of collaboration tools provided under a financially discounted arrangement between NHS Digital and Microsoft with the name N365.

The purpose of this policy is to provide the organisation's statement of intent on how it sets up, secures, uses, and monitors data used on the O365 platform.

It provides staff with their obligations and expectations when using solutions within O365 and helps to reduce the risk associated with use.

This policy will be supported by the available user guides to each of the applications.

Contents

Appendices

See also:
Information Security Policy
Acceptable Use Policy
Policy for the use of Email (NHSMail)
Records Management Policy
Policy for the Photographing and Filming of Patients
Incident Reporting and Management Policy
Social Media Policy

1 Introduction

1.1. Ashford and St Peter's Hospitals NHS Foundation Trust *(hereinafter referred to as the **"organisation"**)* has procured the Microsoft 365 platform under the national NHS discount agreement, named N365, which is made available on a shared tenant platform for NHS customers through an arrangement with NHS Digital.

1.2. For the purpose of this policy and staff familiarity, the term O365 (Office 365) will be used when referring to the N365 shared tenant.

1.3. The O365 platform is a productivity suite of interconnected solutions comprising a set of tools and applications that include, but is not limited to:

- **Microsoft Office** – Outlook, Word, Excel, PowerPoint, OneNote and Access. This includes web-based versions, and, at additional cost, locally installed desktop applications now known as Apps for Enterprise.
- **NHSmail** – Formal messages distributed by electronic means (email). NHSmail is our secure email service, approved by the Department of Health and Social Care for sharing patient identifiable and sensitive information with other NHSmail users and other approved email domains (e.g. Government domains)
- **Microsoft Teams** – A collaboration hub of multiple Teams sites that combines voice and video conferencing with instant messaging (Chat and Posts) and document storage, along with other integrated applications.
- **Microsoft SharePoint** – A website solution that is used as a secure place to store, organize, share, and access information including documents from any device. This is an alternative platform to file shares.
- **Microsoft OneDrive** – A personal drive where personal documents are stored securely in the Cloud to allow easy access from any device, along with secure file sharing. This is an alternative to personal file shares.
- **Microsoft Forms** – An application to create surveys, quizzes, polls, and questionnaires; capture submitted data for presentation in the application or for download.
- **Microsoft Stream** – Cloud video service to create, securely share, and interact, whether in a team or across the organisation. (This functionality is not currently available and is under review with NHS Digital. Meanwhile, recordings of meetings can still be made, and these are stored temporarily within a meeting Chat and are available for download).

1.4. This policy should be read in conjunction with other information security policies, data protection protocols and measures for a complete approach to securing and protecting personal information.

1.5. The organisation recognises the collective solutions that make up the O365 platform are a necessary and standard way to communicate in UK healthcare and makes up an essential part of the organisation's communication with other employees, other NHS organisations, third parties and even our customers.

1.6. Like all forms of technology used by the organisation, the solutions that make up the O365 platform can pose security or business risks if used or set up incorrectly or used inappropriately. This includes the risk of legal action due to breaches of, for example, data protection and confidentiality requirements, threats to IT and information security and ineffective communication. If these risks materialise the organisation and/or the individual employee could be at risk of prosecution.

1.7. This policy sets out our approach and expectations for safe and secure use of the solutions throughout the organisation and provides guidelines on good etiquette for those using and accessing the solutions and the data contained within it.

2 Scope

2.1 This policy applies to all staff within the organisation *(meaning permanent, fixed term and temporary employees, any third-party representatives or sub-contractors, agency workers, volunteers, interns, locums, and agents engaged with the organisation in the UK or overseas).* This also includes staff on secondment, students on placement, external / 3rd party support services staff and people working in a voluntary capacity.

2.2 The policy applies within the organisation premises and outside where staff are using or accessing corporate systems whilst working at home, off-site or travelling.

2.3 This policy is applicable to any device where O365 data is accessed, such as smartphones, tablets, other mobile devices, laptops, desktop computers, etc.

2.4 Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3 Purpose

3.1 The purpose of this policy is to provide the organisation's statement of intent on how it sets up, secures, uses, and monitors data used on the O365 platform. It provides staff with their obligations and expectations when using solutions within O365 and helps to reduce the risk associated with use.

3.2 A portion of the information sent and received by email in the organisation constitutes personal information and as such, this policy should be read in conjunction with our other information security and data protection policies.

4 Explanation of Terms Used

Term	Explanation / Definition
Cloud	A common term used for the internet; Cloud storage refers to information stored on servers that are accessed via the internet.
Data Security and Protection Toolkit (DSPT)	An online assessment tool that enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards.
LOA – Local Organisation Administrator	An employee appointed by the organisation to look after and manage the NHSmail and O365 application accounts and licences.
N365	A suite of electronic productivity tools provided for NHS organisations through an agreement between NHS Digital and Microsoft and based on the Microsoft 365 platform. For the purposes of this document this is referred to as O365.
Shared tenant	A shared environment for NHS organisations using the N365 platform, managed by Accenture on behalf of NHS Digital.

5 Duties and responsibilities

5.1 All Managers

All managers are responsible for:

- reading this policy and ensuring that they understand the contents
- implementing and monitoring the operation of this policy within their functional areas
- ensuring the staff they manage are aware of this policy and their individual responsibility for complying with it
- ensuring that staff are equipped to fulfil their responsibilities as detailed in this policy. This will include coverage at local induction and meeting specific and generic training needs through personal development plans
- identifying staff who have been assigned wider administrative rights and informing the Digital Services department in order that two-factor authentication (2FA) can be initiated. 2FA is mandatory for O365 administrators.

Managers have specific responsibilities at each stage of a staff member's employment:

- Starters – managers should ensure all new staff members, including those not directly employed by the organisation, have read and understood the current version of the Records Management Code of Practice for Health and Social Care
- Movers/leavers – managers will work with a staff member that leaves or changes role to transfer any data stored in O365, including OneDrive, to either an appropriate person or shared work area. This will include ensuring that all person

and organisationally sensitive information is deleted and ensuring that the remaining contents of O365 applications are made available only for future use with another NHS employer (i.e. not for personal use)

- Managers must ensure that Workforce and Digital Services are notified in a timely manner when a staff member, including those not directly employed by the organisation, leaves the organisation, changes department and/or role, or there are any changes to the staff employment status

5.2 All Employees

All staff are responsible for:

- reading and understanding the contents of this policy. Any questions should be raised with a line manager for clarification or escalation as appropriate
- the correct usage of O365 in line with their job role and associated business functions
- ensuring that their account is never used by others and their password is never compromised
- changing the password to access their NHSmail account immediately if they believe that their password has been compromised. This is required because O365 uses NHSmail credentials for authentication
- removing data when it is no longer required in compliance with the organisations' wider data retention policies
- making themselves aware of any Standard Operating Procedures, policy and procedure documents relating to O365 applications
- ensuring that all data containing Patient Confidential Data is retained in the appropriate records management system
- reporting information incidents and near misses, including breaches of this policy, as soon as possible following the Trust Incident reporting policy so appropriate action to rectify can be taken to minimise any potential negative consequences
- where they are employed by two or more NHS organisations, managing their O365 applications to ensure that information and messages relating to separate NHS employers are handled appropriately and that any information contained within communications is separated accordingly

5.3 Digital Services

The Digital Services team is responsible for:

- providing access to O365 applications and ensuring that access is compliant with the Data Security and Protection Toolkit standards
- administering O365 accounts in accordance with local procedures and to provide support in the use of O365 applications

- monitoring inactive accounts and taking appropriate action
- providing guidance on O365 applications use to ensure compliance with NHS standards, organisational policy, and any relevant legislation (e.g. UK law and GDPR)
- providing information from an individual's O365 account when requested to support an official investigation
- assisting with providing access in the absence of a staff member for business continuity purposes, where appropriate approval has been given, and to ensure that access is provided in line with this policy
- facilitating requests for forensic discovery audits in the event of a formal investigation and to ensure that these are provided in line with this policy

5.4 O365 Specific Roles: Administrators, Owners, Members and Guests

It is important to understand the different roles that are available on the O365 platform as staff can take the part of multiple roles for multiple applications.

5.4.1 Administrators

Administrators are typically members of the **Digital Services department** and control overall access to the platform.

Administrators are responsible for:

- managing user accounts alongside the Workforce and Development department as part of the joiners/movers/leavers process (JML)
- managing Guest accounts for people accessing the platform from external organisations in accordance with Trust policy and process for 3rd party access
- setting up and removing SharePoint and Teams Sites
- allocating appropriate licenses to users as required
- managing license policies
- providing support to the platform and escalating support to national teams as required
- ensuring that their account is enhanced with two-factor authentication (2FA)

5.4.2 Owners

Owners are required when a SharePoint Site, Teams Site, or Private Teams Channel is set up.

Owners are typically not members of the Digital Services department, but have some administration access and privileges such as the ability to:

- add or remove members
- delete conversations

- change limited settings about the site/channel
- rename the group
- update the description or picture

Owners are responsible for:

- the veracity of information stored within the site they own
- controlling membership access and security permissions, including the management of users to create and update channels in Teams
- ensuring that access membership and security permissions are regularly reviewed
- following best practice use of all applications

Owners can be changed as needed over time in line with organisational changes.

5.4.3 Members

Members are users within the organisation who have been added to SharePoint Sites, Teams Sites, or Private Teams Channels by the owner.

Members can use all the functions to collaborate on the platform and have access to everything granted to them by owners, however, they cannot change settings.

Members are responsible for:

- ensuring that any data or content that forms part of a record is copied from the O365 application and uploaded to the relevant record management system (e.g. the electronic patient record)
- following best practice use of all applications

5.4.4 Guests

Guests on the shared tenant platform are defined as anyone not using their NHSmail account (nhs.net) to access the platform.

Guests can be other NHS organisations that have not joined the shared tenant and are using their own dedicated O365 tenant platforms (typically their email address ends with '.nhs.uk'). Guest access lets staff collaborate with experts, partners, vendors, suppliers, and consultants outside of the organisation.

Guests are responsible for:

- ensuring that any data or content that forms part of a record is copied from the O365 application and uploaded to the relevant record management system (e.g. the electronic patient record)
- following best practice use of all applications

6 Policy

6.1 Standards and Practice

This policy is based on current legislation, NHS information governance standards and accepted standards of good practice. Employee's duty to handle organisation and personal identifiable data appropriately arises out of common law, legal obligations, employment contracts and professional obligations.

Any breaches of this policy may result in the employee's employment being terminated. It may also bring into question any professional registration and may result in disciplinary, civil, or criminal proceedings.

Messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant to the issues. The content of any messages may be disclosed under the Data Protection Act 2018, Freedom of Information Act 2000, and the Environmental Information Regulations 2004. Therefore, the author must ensure the content, style and language used is appropriate, as any data subjects mentioned may legally request access to the messages as a Subject Access Request under the Data Protection Act.

If there is anything that is not clear or the employee does not understand in this policy, they must contact their line manager in the first instance, or the Information Governance Manager for further information.

6.2 Changes to Employment Status

When an employee has their employment status changed to inactive the manager should notify the IT Service Desk to ensure that the corresponding account is managed appropriately.

Staff on secondment to another NHS organisation should be treated as a leaver and joined to the seconded organisation within 30 days.

Where an employee has employment with two or more NHS organisations, the substantive or earliest employer will determine the default organisation that their named O365 account will be associated with.

6.3 O365 – Use and Guidelines

The O365 platform comprises a suite of interconnected productivity solutions, tools, and applications.

6.3.1 O365 – Acceptable Use

The organisation has adopted a set of acceptable use guidelines for staff to follow when using all solutions on the O365 platform:

- Access is provided for staff for work duties and work-related educational purposes

- Data must be used and controlled in accordance with current legislation, regulations, and local Trust policies, including the Information Security Policy
- Staff must always adhere to this policy when using any solution within the O365 platform
- Data from the O365 platform should not be downloaded to the local storage on personally owned devices under any circumstances
- Staff must only access their own O365 accounts and must not share or disclose logins or passwords
- No employee has the right to an O365 account. On this basis the inappropriate use or abuse of an O365 account provided by the organisation may result in access being withdrawn or suspended

6.3.2 O365 - Best Practice

The organisation advises that when using the applications within the O365 platform, staff should:

- When accessing any O365 data (NHSMail email, Teams, SharePoint, OneDrive, etc.) from a non-NHS device (e.g. a personally owned laptop, tablet, smartphone, etc.), users **must not** download any data
- Minimise the use of confidential person identifiable data (PID)
- Remember that the O365 platform **is not** a records management system. Where the content may be needed in the future it is the responsibility of the owner / organiser to ensure data is stored appropriately within the relevant record management system
- Where content on the platform forms part of a record stored elsewhere, it is the responsibility of the user to ensure that the record is updated with the additional information, and that it becomes part of that record going forward. The following examples are where information may need to be copied from an O365 platform application into a record management system. This list is not exhaustive:
    - MS Teams chats
    - Email content, including any data contained in an attachment
    - Information recorded / noted from a Teams voice and/or video meeting

6.4 NHSmail – Use and Guidelines

NHSmail is the national secure collaboration service for health and social care in England and forms part of the O365 platform.

Staff should refer to the Trust Policy for the use of Email (NHSmail) for all guidance relating to the use of NHSmail.

6.5 Microsoft Teams - Use and Guidelines

Microsoft Teams is a collaboration hub of multiple Teams sites that combines voice and video conferencing with chat, instant messaging, and document storage, along with other integrated applications.

Teams sites are collections of people who gather around a common goal and are typically organised around departments or functions. However, there will be sites that are common across departments, functions and even organisations.

The creation and deletion of Teams sites is managed by the Digital Services team and all Teams sites **must** be set to Private when created. Failure to do so will make the Team, and all data within it, available across the whole NHS shared tenant.

Within Teams sites, Channels can be created to enable more focussed group conversations, support dedicated discussion topics, and to provide sources of expertise.

There are two types of Channel:

- **Standard Channel:** available and visible to everyone who is a member of the parent Teams site.
- **Private Channel:** a focused private area with access granted only to selected members of the parent Teams site. A member of a private channel must be a member of the parent Teams site.

Channels can be named when created, but the General channel is created by default with the Teams site and cannot be changed. The General channel essentially acts as the central Teams site message board.

6.5.1 Microsoft Teams - Acceptable Use

The organisation has adopted the below set of acceptable use guidelines for staff to follow when using the Microsoft Teams solution:

- The organisation Teams communications should only be used for legitimate business use and in accordance with the Trust Information Security Policy
- MS Teams is a secure system that can be used when necessary to share sensitive personal information. However, before doing so, please discuss with your line manager, or seek advice from the Digital Services or Information Governance teams, to ensure adherence to the relevant Trust policies and guidelines relating to data security and protection
- Demonstrate respect and consideration for colleagues in any messages sent using MS Teams

6.5.2 Microsoft Teams – Best Practice

Communication with others using Microsoft Teams (MS Teams) is more informal than email and letters, and may feel less permanent, but applying the same care and consideration given to emails is expected.

The organisation advises that when using MS Teams, staff should:

- take note of other users' status updates as a common courtesy and to ensure effective communication
- ensure Teams meeting recipients are bcc'd in if you wish to their hide contact details
- take care to maintain a professional attitude during calls and to be mindful that others may not be as comfortable and may find video calls intrusive or disconcerting
- be mindful that files and information made available through Teams may remain available indefinitely, depending on how individuals are included in any meeting or chat
- be aware where any shared files are stored:
    - files for formal Teams sites and channels are stored in SharePoint
    - files in standalone meetings, ad-hoc calls, or chats will be stored in the sharers OneDrive for the person sharing the file
- ensure that a Teams meeting created for one purpose is not reused for another, e.g. senior management meeting and then reused for an all staff meeting, leading to risk of inappropriate access to shared messages and documents.
    - The **Web Link (URL)** provided when creating a Teams meeting **is unique** and is the "secure access key" to the meeting. Sharing this key allows any recipient to access the meeting once they have it. If this is a repeating meeting, then a guest invited just once will always see the meeting chats and documents shared to the meeting as future meetings take place. They can join the subsequent meetings any time they wish
    - If repeat meetings are needed where guests may need to join from time to time, send a place holder meeting without the Teams link and create the unique teams meeting request for each meeting to accompany the place holder meeting
- adjust the meeting options, where Teams is being used for sensitive or confidential discussions, so that **only the meeting organiser can bypass the lobby** and everyone else is forced to wait in the online lobby before joining. The meeting organiser can then selectively bring people in as needed. The Teams meeting organizer needs to:
    - Select the Meeting Options web link in the Teams meeting invitation, then adjust the "Who can bypass the lobby" option to "Only Me", as well as any other meeting security options
- use the organisation's recommended solution for direct patient video consultations, only using Teams where the recommended solution is not possible or appropriate

- consider that the use of Teams chat is mostly for brief and interactive communications and that formal communications may still require an email
- be aware that if a Teams meeting is created from within the Teams application rather than Outlook, then a Teams Channel can be added to the meeting. If this is done, all members of that channel will be invited to the Teams meeting. They will also see any chats, or files generated before, during or after a meeting
- be aware that it is the responsibility of all staff to remove Teams data they control when it is no longer required, in compliance with the organisations wider data retention policies

6.5.3 Microsoft Teams – Screen Sharing Best Practice

- Teams provides the ability for any user to share their screen, presentation, or application as part of a meeting, either scheduled or ad hoc. It is very important that staff are aware of what could potentially be presented when sharing content in a meeting

- Sharing a screen will show everything on that screen to all meeting participants. If the presenter switches to another app on the same shared screen, its contents will be also displayed to the participants

- Consider sharing an application or a specific presentation instead

- Where more than one screen is used, it is recommended to move the content and apps whose content are being presented to one screen. This avoids the need for extra adjustments during the meeting and reduces the risk of sharing the wrong information

- Prepare in advance before a meeting to make sure you have easy access to the files you need, set up your computer for screen sharing and queue up your first document

6.5.4 Microsoft Teams - Videocalls and Videoconferencing – Acceptable Use

The video call and conference facility in Teams can be used in all scenarios that could be conducted in person in a physical location, except for direct patient video consultations, which should be undertaken using the organisation's recommended solution.

It is acceptable to use background blur or an appropriate background image. This is especially recommended if in a sensitive area where the background should not be visible.

All recordings involving patients must be in accordance with the Trust policy for Photographing and Filming Patients.

6.5.5 Microsoft Teams - Videocalls and Videoconferencing – Best Practice

The organisation expects video calls to operate standards like physical meetings, there are however some additional considerations:

- The participants should be aware of who is present in a meeting and act in an appropriate manner

- Staff must try to avoid being overheard by having calls in private, particularly when confidential information is being discussed

- Staff should endeavour to attend meetings promptly and avoid over-running

- Participant microphones should be muted initially, especially on group calls

- Staff are encouraged to switch on cameras during videocalls but are not obliged to

- All pertinent information arising from the call should be added into the relevant business or patient records as soon as possible after a call. The person(s) responsible for this should ideally be agreed at the start of the call

- Where it is necessary to record a video call this must be stated before recording starts. This provides an opportunity for objections to be made and concerns respected and possibly acted upon. This potentially could involve individuals turning off their camera. Alternatively, individuals may wish to withdraw from the meeting

- Staff should be aware that with recordings the general approach is that they are not the final formal record of information to be kept and will be deleted when no longer required. If a decision is made to use call recordings as the main record, then appropriate steps must be taken to catalogue and protect them the same as any other information

- Staff should be aware of their surroundings, including what may be shown in the background, and use the blur or background picture options as appropriate, but should not use applications or settings that filter or change appearances

- When someone other than the presenter wishes to speak, they should raise their hand to speak unless specified otherwise at the start of the meeting. The presenter or nominated person during the meeting should maintain awareness of participants raising their hands via the meeting participant's tab

- Consider the use of Live Captions. If an attendee in a meeting is hard of hearing, isn't a native English speaker, or is having trouble hearing the audio for another reason, Teams' built-in closed captioning feature can help them follow the conversation better. It automatically converts speech into captions that appear below the video feed in real time

- The use of the Transcription facility is permitted. Staff should be aware that accuracy is not optimal and this should not be considered an accurate record of a meeting.

6.6 Microsoft SharePoint – Use and Guidelines

SharePoint is a document management system and web portal that allows information to be collated and shared as web pages, lists, stored files, databases, etc.

6.6.1 SharePoint – Acceptable Use

SharePoint sites must only be used for legitimate business purposes.

6.6.2 SharePoint – Best Practice

The organisation advises that when using SharePoint, staff should:

- always be mindful that this is an internet connected application that promotes sharing, and consider the risk of confidential information being shared inadvertently when using the platform
- notify the Information Governance team in advance when there is a requirement for a SharePoint site to contain confidential information, or where a SharePoint site is to be shared with other organisations, as it may need to be included on the Information Asset Register and may require the completion of a Data Protection Impact Assessment (DPIA)
- Ensure that data is retained in accordance with the organisation's data retention policies

6.7 Microsoft OneDrive - Use and Guidelines

Documents saved to OneDrive are stored securely in the Cloud. Information stored on OneDrive meets security requirements in that it is encrypted both in transit and at rest.

Files stored in OneDrive may be synchronised with your NHS PC and vice versa and may be shared securely with other O365 users.

6.7.1 OneDrive - Acceptable Use

The organisation has adopted the below set of acceptable use guidelines for staff to follow when using OneDrive. Appropriate use of OneDrive is essential to the organisation's reputation.

- OneDrive should only be used to store personal business information. Information relating to the department or team should be located on the departmental or team network drives, SharePoint sites or Teams sites as appropriate, unless the information is deemed to be of a confidential nature, such as staff appraisals, etc.
- OneDrive should be used in the same manner as a personal network drive (H:\ drive)
- Staff must keep data storage to a minimum and delete obsolete files on a regular basis in compliance with the organisation's wider data retention policies
- It is imperative that all data containing Patient Confidential Data is retained in the appropriate records management system in accordance with the organisation's data retention policies

6.7.2 OneDrive - Best Practice

The organisation advises that when using OneDrive, staff should:

- not set up permissions to provide “Allow everyone in your company”, “Public” or “Organisation Wide” access
- ensure that when leaving a post that all appropriate OneDrive data is transferred to an appropriate colleague as agreed with their line manager or head of department
- use OneDrive to store documents and/or other data on the device provided to you by the organisation. Data stored locally (e.g. C: drive) on a desktop computer, laptop, or mobile device are not backed up and may be irretrievably lost if the device fails or is stolen
- be aware that the data contained in a OneDrive account **may** be deleted when an employee leaves the organisation.

6.8 Microsoft Forms – Use and Guidelines

Forms provides functionality to create surveys, quizzes, polls, and questionnaires, with data being accessible immediately on submission to produce real-time charts within the Forms application or to be downloaded and manipulated through another application.

6.8.1 Microsoft Forms – Acceptable Use

The organisation has adopted the below set of acceptable use guidelines for staff to follow when using Forms. Appropriate use of Forms is essential to the organisation’s reputation.

- Forms must only be used for legitimate business use
- Where the capture of personal identifiable information is intended, a data protection privacy impact assessment (DPIA) must be completed in advance
- Data storage must be kept to a minimum, and obsolete files must be deleted on a regular basis in compliance with the organisation’s wider data retention policies
- It is imperative that all data containing patient confidential data is retained in the appropriate records management system in accordance with the organisation’s data retention policies

6.8.2 Microsoft Forms – Best Practice

The organisation advises that when using Forms, staff should:

- consider the appropriateness of questions and the intended audience
- consider the requirements for data capture and data retention

6.9 Reporting Incidents

All staff are responsible for reporting incidents of unacceptable use, information incidents and near misses, including breaches of this and any other policy.

Significant Cyber-Security or Data Protection breaches must also be reported to the national bodies via the DSP Toolkit within 72 hours. Please contact the Digital Services and Information Governance teams in such circumstances as soon as possible.

Any instances of suspected fraud should be referred to the Local Counter Fraud Specialist.

All incidents should be reported in line with the Trust Incident Reporting and Management Policy.

6.10 Use of Personally Owned Devices

The O365 platform is accessible from any internet connected device. However, there are certain conditions that must be adhered to when accessing data from a personally owned device and these are:

- use of personally owned devices must be in accordance with the Information Security Policy
- data from the O365 platform should not be downloaded on to personal devices under any circumstances

6.11 Liability

The organisation will not be liable for any financial or material loss to an employee when using O365 applications for personal use or when using personally owned equipment to access their organisation O365 account.

6.12 O365 Archiving and Retention

Under the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA18), all personal data is subject to minimisation and storage limitation principles.

All areas and applications within O365 are subject to these principles.

Retention on the O365 shared tenant is set at a national level by NHS Digital and is subject to amendment and change. A comprehensive and current list can be found here: Data Retention and Information Management Policy – Office 365 – NHSmail Support

For emails, archive messages and OneDrive, data is stored if the account is active, and the data is not deleted. An account will remain active if it has been logged into, had a password change, or sent an email within the last 365 days.

For O365 applications such as Teams and SharePoint, data is stored until either the data is specifically deleted or the sites containing the data are deleted.

All deleted data falls under retention policies which maintain data in its deleted state for 180 days since last edited, before permanently removing the data.

Any data sent or received through the O365 system forms part of our organisation business records and must be retained in accordance with the Trust Records Management Policy. Where the content of a message forms part of a record it is the responsibility of the employee to ensure it is added to, and becomes part of, that record, whether held in hard copy or electronic format.

The organisation reserves the right to retain any information and/or messages as required to meet its legal obligations.

6.13 O365 Monitoring

The systems, software and applications provided as part of O365 are licenced for employees' lawful use and as such will be subject to monitoring. Activity monitoring and data loss prevention tools are available and will be used to ensure compliance with legislation.

Any monitoring or interception of communications will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 2018, the General Data Protection Regulation, the Human Rights Act 1998 and specific procedures around monitoring and privacy.

6.14 Access to O365 Applications and Accounts in the Event of an Investigation

It may be necessary in the course of an official investigation, such as formal HR disciplinary investigations, investigations by or on behalf of the Police or the Counter Fraud Specialist, to give access outside of the normal line management arrangements to messages or files stored in O365 in conjunction with the NHSmail Access to Data Procedure. Any official investigations will be carried out in accordance with the legislation described in section 6.13 above.

Investigation requests relating to an employee's account will only be accepted from the relevant HR Business Partner, the appointed investigating officer, or the Local Counter Fraud Specialist.

Investigation requests must be made in writing via email to the Director of Digital and contain the explicit permission of the requesting officer as outlined above.

If the information to be returned to the investigation contains personal identifiable data, this information must be handled appropriately, maintaining confidentiality always.

Staff should be aware that requests relating to MS Teams accounts may return all communication pertaining to the request, including details of any communications which have been deleted.

7 Training and Support

The use of some components of O365 may be familiar to some staff, therefore training will be offered as optional.

A blended learning approach is available using videos, how to guides and face to face training delivered over MS Teams.

Training will be provided by Digital Services IT Training team where required.

General support will be available through the IT Service Desk.

Support or queries regarding confidentiality aspects of information being stored or sent should be raised to the Information Governance Team asp-tr.IG@nhs.net .

8 Stakeholder Engagement and Communication

This policy has been developed following guidance from NHS Digital and the NHS N365 shared tenant national team, with the involvement of the Trust Digital Services department, the Trust O365 project team and the members of the Information Governance Steering Group.

9 Approval and Ratification

The policy will be approved and ratified by the Information Governance Steering Group.

10 Dissemination and Implementation

The policy will be disseminated through the Aspire global email and published on the organisation intranet and internet sites.

The Information Governance Steering Group is responsible for the implementation of this policy, including monitoring compliance.

11 Review and Revision Arrangements

This policy will be reviewed every 3 years in line with Trust policy or updated in line with any new legislation issued or change in procedures.

12 Document Control and Archiving

This is a Trust-wide document and archiving arrangements are managed by the Quality Department, which can be contacted to request master/archived copies.

13 Monitoring compliance with this Policy

Measurable Policy Objective	Monitoring/ Audit method	Frequency of monitoring	Responsibility for performing the monitoring	Monitoring reported to which groups/ committees, inc. responsibility for reviewing action plans
Appropriate licence assignment	Licence Allocation Report	Quarterly	Local Organisation Administrators (LOAs) in the Digital Services Team	Information Governance Steering Group
Records archiving and retention	One Drive Consumption Report	Quarterly	Local Organisation Administrators (LOAs) in the Digital Services Team	Information Governance Steering Group

14 Supporting References / Evidence Base

Caldicott Principles
https://www.ukcgc.uk/manual/principles

Common law duty of confidentiality
https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality

Computer Misuse Act 1990
https://www.legislation.gov.uk/ukpga/1990/18/contents

Confidentiality: NHS Code of Practice
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Data Protection Act 2018
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Environmental Information Regulations 2004
https://www.legislation.gov.uk/uksi/2004/3391/contents/made

Freedom of Information Act 2000
https://www.legislation.gov.uk/ukpga/2000/36/contents

Human Rights Act 1998
https://www.legislation.gov.uk/ukpga/1998/42/contents

NHSmail Acceptable Use Policy
https://support.nhs.net/knowledge-base/acceptable-use-policy/

NHSmail Access Policy
https://support.nhs.net/knowledge-base/access-policy/

NHSmail Data Retention and Information Management Policy
https://support.nhs.net/knowledge-base/nhsmail-data-retention-and-information-management-policy/

Records Management Code of Practice for Health and Social Care
Records Management Code of Practice for Health and Social Care 2016 - NHS Digital

APPENDIX 1: EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Summary

Name and title: Nicki Rayment – Head of Digital Programme Delivery
Policy: O365 Acceptable Use Policy

Background • Who was involved in the Equality Impact Assessment
Staff from Digital Services, members of the Digital Programme Steering Group and members of the Information Governance Steering Group.
Methodology • A brief account of how the likely effects of the policy were assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age) • The data sources and any other information used • The consultation that was carried out (who, why and how)
The policy was assessed as not impacting upon an individual's race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age. The information was a review of policy itself.
Key Findings • Describe the results of the assessment • Identify if there are adverse or potentially adverse impacts for any equalities groups
No adverse or potentially adverse impacts have been identified for any equalities groups; the policy affects all staff equally.
Conclusion • Provide a summary of the overall conclusions
No adverse or potentially adverse impacts have been identified for any equalities groups; the policy affects all staff equally.

Recommendations • State recommended changes to the proposed policy as a result of the impact assessment • Where it has not been possible to amend the policy, provide the detail of any actions that have been identified • Describe the plans for reviewing the assessment
No changes recommended.

Appendix 2 - Quick Guide to Acceptable Use