Document Type:	Policy Guideline	
Reference Number : **SDHIS-N365-1**	Version Number: **1.1**	Next Review Date: **01-07-2025**
Title:	**Microsoft 365 Services Platform – Policy**	
Document Owner:	N365 Platform IAO	
Applicability:	LA, Microsoft Teams Owners and Users of the N365 platform.	

Document Control Information

This is a controlled document and should not be altered in any way without the express permission of the author or their representative.

Please note this document is only valid from the date approved below, and checks should be made that it is the most up to date version available.

If printed, this document is only valid for the day of printing.

This policy has been registered with the Trust. The interpretation and application of guidance will remain the responsibility of the individual clinician. If in doubt, contact a senior colleague or expert. Caution is advised when using clinical guidance after the review date, or outside of the Trust.

Ref No:	SDHIS-N365-1		
Document title:	Microsoft 365 Services Platform Policy		
Purpose of document:	Terms of usage		
Date of issue:	15-06-2022	**Next review date:**	01-07-2025
Version:	1.1	**Last review date:**	17-08-2022
Author:	Phil Sweet		
Directorate:	SDHIS		
Equality Impact:	The guidance contained in this document is intended to be inclusive for all patients within the clinical group specified, regardless of age, disability, gender, gender identity, sexual orientation, race and ethnicity & religion or belief		
Committee(s) approving the document:	IM&T Group		
Date approved:	14th June 2022		
Links or overlaps with other policies:	**Mobile Phone Policy V4**		
	NHSmail Acceptable Use Policy (AUP)		
	IT Procedure – Microsoft 365 Services Platform		

Document Amendment History

Date	Version no.	Amendment summary	Ratified by:
19-01-2022	0.1	Draft	Phil Sweet
11-05-2022	0.2	Changes to add recent additions to the platform	Phil Sweet
27-05-2022	0.3	Incorporating comments from IT Director	Phil Sweet
01-06-2022	0.4	Additional feedback received	Phil Sweet
08-06-2022	0.5	Local feedback signed off and ready for IM&T approval	Phil Sweet, Gary Hotine & Jai Ragwani
14-06-2022	0.6	Edit made per IM&T Group feedback to reflect that N365 services can be used for private patient activities	Jai Ragwani & IM&T Group
15-06-2022	1.0	Approved by IM&T Group on 14th June 2022	IM&T Group
17-08-2022	1.1	Minor amendments to MS Forms section to clarify use of existing survey technologies and IG related responsibilities of individual Forms users as agreed with IG Lead.	Jai Ragwani

Contents

0.1 Policy Statement

Torbay and South Devon Foundation Trust *(hereinafter referred to as the **"organisation" or "Trust")*** has procured and makes available the Microsoft 365 platform signed under the national discount agreement known as N365 for our employees in the functioning of our organisations activities but recognise the risks to security and personal data posed by such use. The N365 platform is a productivity suite of interconnected solutions comprising of tools and systems that include, but are not limited to:

- **Microsoft Office** - Outlook, Word, Excel, PowerPoint, OneNote, Access (which includes web-based cloud versions and locally installed applications now known as Apps for Enterprise).
- **NHSmail (Exchange Mail)** - 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.
- **Microsoft Teams** - A collaboration hub of multiple Teams sites that combines voice and video conferencing with WhatsApp style chat, instant messaging, and document storage 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.
- **Microsoft Stream** - Cloud video service in Office 365 - makes it easy to create, securely share, and interact, whether in a team or across the organisation.
- **Microsoft Whiteboard** - The collaborative digital canvas in Microsoft 365 for effective online and hybrid meetings and engaging learning.
- **Power Automate** - Streamline repetitive tasks and paperless processes so you can focus your attention where it's needed most.
- **Power Apps** - Easily develop mobile and web apps for any business need—even if you have no technical or development experience

This policy should be read in conjunction with our other information security policies, data protection protocols and measures for a complete approach to securing and protecting personal information.
The organisation recognises the collective solutions that make up the N365 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.
Like all forms of technology used by the organisation, the solutions that make up N365 platform can pose security or business risks if used or set-up incorrectly or inappropriately. 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.

0.2 Purpose

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 N365 platform. It provides employees with their obligations and expectations when using solutions within N365 and helps to reduce the risk associated with corporate use of the platform.

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.

0.3 Scope

This policy applies to all staff within the organisation *(meaning permanent, fixed term, and temporary staff, any third-party representatives, or sub-contractors, those with honorary contracts, 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.

The policy applies within the organisation premises and outside where employees are using or accessing corporate systems whilst working at home or travelling.

This policy is applicable to any device where N365 data is accessed, including smartphones, tablets, other mobile devices, laptops, and desktop computers.

Adherence to this policy is mandatory.

Non-compliance could lead to disciplinary action up to and including summary dismissal.

1 N365 Platform Guidelines

The N365 platform provides flexible and powerful systems and tools of great benefit to the organisation when used appropriately. Their use, however, also exposes the organisation and individual users to new risks. These include legal action due to breaches of data protection and confidentiality requirements, threats to IT and information security, and ineffective communication. These risks and threats can compromise the organisation's ability to deliver effective care and services.

The organisation has set out the following guidance for employees on how to use all the solutions within the N365 platform for best practice, acceptable use and any actions deemed unacceptable when using or accessing the organisation data on the platform. The N365 solution has been adopted by the organisation and it meets a set of information security controls that offer an appropriate level of protection against loss or inappropriate access. Microsoft Office 365 is operated and used in accordance with a set of national policies and procedures:

- Microsoft Teams Apps Security and Compliance - NHSmail Support
- Policies - NHSmail Support

The following sections set out guidance across the N365 platform generally. Specific applications/solutions are detailed further in this document to provide more specific guidance as an additional layer to the general platform guidelines.

1.1 Roles - Administrators, Owners, Members and Guests

It is important to understand the different roles that are available on the N365 platform as staff can take the part of multiple roles on the platform. Please refer to the Procedure document for detail on role responsibility.

1.2 Acceptable Use

The organisation has adopted the below set of acceptable use guidelines for employees to follow when using all solutions in the N365 platform (including all of Teams, SharePoint, and OneDrive):

- Data in the N365 platform must be used in accordance with current legislation and regulations.
- Employees must adhere to this policy at all times when using any solution within the N365 platform.
- For Trust owned devices: All access to the platform including local file storage is permitted, however it is preferred for all files to remain in the N365 platform (OneDrive, Exchange Mail, Teams, or SharePoint), rather than on the physical device.
- For personally owned devices: Files stored/accessed in the N365 solution should NOT be downloaded/copied on to personal devices; however, we DO encourage, and support files accessed from the N365 solution that are opened/accessed and viewed/edited on a personal device. Further guidance is available in the N365 Procedure document, or advice can be sought from the TSDFT N365 support team via the Service Desk.

- Employees must only access their own accounts and must not share or disclose logins or passwords.

1.3 Prohibited Use

In addition to the acceptable use of the N365 platform, the below actions and forms of use are unacceptable and must NOT be used by any employees:

- To send or receive inappropriate content or attachments, including distributing, disseminating, or storing images, text or materials that might be considered indecent, racist, sexist, abusive, offensive, pornographic, obscene, or illegal.
- Create, hold, send or forward emails and messages that contain statements that are untrue, inaccurate, misleading, or offensive about any person, the NHS, or the organisation.
- To disseminate personal contentious views or opinions, or for personal gain (other than legitimate private patient activities).
- For sharing confidential data to any unauthorised person/organisation.
- Forwarding of Trust confidential/commercially sensitive data to external organisations.
- To send, receive or access any copyrighted information in a way that violates or breaches that copyright.
- To engage in any illegal activities.
    - Discovery of such material shall, if deemed as being of a criminal nature, be reported to the police.
- In a way that restricts the sharing or access of files by other employees, or for undertaking deliberate activities that deny IT infrastructure resources.
- In a way that could be expected to introduce any form of computer virus or malware into the Trust's network.
    - For Example, knowingly upload malicious software to Teams, or SharePoint Online, or send an email with a known malicious attachment.
- To access and use another user's account without permission. If it is necessary to access another user's account, then contact the **Service Desk** for details of the necessary procedure (users should be aware that access to their email/N365 account by authorised individuals may be necessary in periods of absence for business continuity reasons).
- To forge or attempt to forge email messages, for example, spoofing.

1.4 Multi-Factor Authentication (MFA)

Staff who have been assigned wider administrative rights, have access to confidential/sensitive information or intend to use the solution on a personal device will have their account security enhanced by enabling multi-factor authentication. The N365 team may apply MFA to any account, at any time, and for any period.

1.5 Legal Requirements

The use of the N365 platform must comply with the law such as the Data Protection Act 2018 and the UK-GDPR and adhere to Trust codes of conduct, policies, and procedures such as this policy, and policies relating to equalities and anti-harassment.

- Users must comply with any licence conditions and copyright for any software they have access to.
- Users must not use the N365 platform or associated systems for any purpose that conflicts with their contract of employment.
- Users must not agree to terms or enter into contractual commitments or make representations by email or MS Teams, without having obtained the proper authority (a typed name at the end of an email is just as much a signature as if it had been signed on paper).
- Emails and MS Teams messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant.
- The content of any messages may be disclosable under legislation such as the Data Protection Act 2018 / UK-GDPR and Freedom of Information Act 2000.
- Improper statements may result in the organisation and/or user being liable under law.

1.6 Reporting Incidents

- All Staff must report serious incidents of unacceptable use, for example, obscene or racially offensive emails to their line manager or, where this is not possible, log an incident on Datix. If in doubt, contact the **Information Governance department** for advice.
- All staff are responsible for reporting information incidents and near misses, including breaches of this and any other policy. They should be reported in line with the Incident Reporting Policy.
- Significant Cyber-Security or Data Protection breaches must also be reported to the national bodies via the DSP Toolkit within 72 hours (www.dsptoolkit.nhs.uk). Please contact the **Service Desk** and the Information Governance department in such circumstances **as soon as possible.**
- Any instances of suspected fraud should be referred to the **Local Counter Fraud Specialist**.

1.7 Personally Owned Devices

Please refer to the organisation's *Bring Your Own Device (BYOD) Policy*, however section 1.2 applies more specifically to the N365 platform.

2 NHSmail - Email Specific Guidance

The organisation has set out guidance for employees on how to use email for best practice, acceptable use and any actions deemed unacceptable when using or accessing the organisation email. NHSmail has been adopted by the Trust and it meets a set of information security controls that offer an appropriate level of protection against loss or inappropriate access. Emails sent to and from health and social care organisations must meet the secure email standards (DCB1596). NHSmail is operated and used in accordance with a set of clear policies and procedures, with detailed information on its use: https://support.nhs.net/article-categories/policy/

2.1 Personal Email

The organisation understands that email forms a large part of individual's daily life and is an integral communication tool used by most people. As such, we allow the accessing of personal email, with the below stipulations:

- Employees must never use personal email to send or receive material or information relating to or owned by the organisation or for business purposes.
- Personal email must never be used to send or receive inappropriate content, whether for personal or business purposes.

3. Microsoft Teams Use

Microsoft Teams is a collaboration hub of multiple Teams sites that combines voice and video conferencing with WhatsApp style chat, instant messaging, and document storage with other integrated applications. Teams sites are collections of people who gather around a common goal. Most team sites will be around departments, however, there will be sites that are common across both departments and organisations. Within Teams sites, you can have Channels, which enable more focused group conversations.

3.0.1 Prohibited Use

In addition to the acceptable use and policies set out nationally, the below actions and forms of use are unacceptable.

Microsoft Teams must NOT be used:

- For sending confidential messages to any unauthorised person or organisation.
- For sharing of organisation confidential data to external organisations/people.
- To send, receive or access any copyrighted information in a way that violates or breaches that copyright.

- In a way that could be expected to introduce any form of computer virus or malware into the organisation network.

3.1 SharePoint

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

3.1.1 Acceptable Use

The organisation has adopted the below set of acceptable use guidelines for employees to follow when using the Microsoft SharePoint solution: -

- The organisation SharePoint site should only be used for legitimate business use.
- The availability of an application/add-in on the platform does not constitute authorisation to use it within the organisation. Users are responsible for ensuring apps/add-ins are approved for Trust use before using them. Please consult the Service Desk if required.
- SharePoint Site owners are responsible for:
    - The veracity of information stored within it
    - Controlling membership access and security permissions
    - Ensuring that access membership and security permissions are regularly reviewed.

3.1.2 Best Practice

The organisation suggests that when using Microsoft SharePoint, employees <u>should</u>:

- Always be mindful that this is an internet connected application which promote sharing and consider the risk of confidential information being shared inadvertently when using the platform.
- Notify the Information Governance department when there is a requirement for a SharePoint site to contain confidential information or where a SharePoint is shared with other organisations, as it may need including on the Information Asset Register as well as completion of a DPIA.
- It is the responsibility of all staff to remove SharePoint data they control when it is no longer required, in compliance with the organisation's wider data retention policies.
    - It is imperative that all data containing Personal Identifiable Data is retained in the appropriate records management system in accordance with our Retention Periods schedule.

3.2 OneDrive

Documents saved to Microsoft 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.

3.2.1 Acceptable Use

The organisation has adopted the below set of acceptable use guidelines for employees to follow when using OneDrive:

- Files relating to the department should be located on the departmental SharePoint/Teams Sites as appropriate. OneDrive is an alternative product to store private data/sensitive files that are being worked on in draft, that can be shared with individual colleagues. Guidance on use is available in the N365 procedure.
- Staff must keep data storage to a reasonable level and delete obsolete files. It is the responsibility of all staff to delete files that are no longer required in compliance with the organisation's wider data retention policies. Any account with excessive storage levels may be contacted and asked to initiate housekeeping procedures for file storage. The global storage levels will be reviewed as part of the N365 funding reviews. If additional licences are required to support larger storage, then this cost may be recharged to the relevant department.
    - The N365 platform should NEVER be used as the sole repository for PID. It is imperative that all data containing Personal Identifiable Data is retained in the appropriate clinical system/admin management system, in accordance with our Retention Periods schedule.

3.2.2 Prohibited Use

In addition to the acceptable use and policies set out nationally, the below actions and forms of use are unacceptable.

- Employees shall not use any other Internet-based file sharing applications such as DropBox, unless explicitly approved and provided as a service by SDHIS.

3.3 Microsoft Stream

Microsoft Stream enables live streaming and video on demand (VOD) for team meetings, events, and training. It is a secure repository to enable staff to upload and share video content.
In addition to the acceptable use and policies set out nationally and as outlined above under the platform guidelines, the organisation has adopted the below set of acceptable use guidelines for employees to follow when using the Microsoft Stream solution: -

- The Microsoft Streams solution should only be used for legitimate business use.
- All participants to a video recorded and saved into teams must be aware and willing to be

recorded.

- It is the responsibility of all staff to remove streams data they control when it is no longer required, in compliance with the organisation's wider data retention policies.
    - It is imperative that all data containing Personal Identifiable Data is retained in the appropriate records management system in accordance with our Retention Periods schedule.

3.4 Microsoft Forms

Microsoft Forms provides the ability for staff to create surveys, quizzes, polls, and questionnaires, then make real time automatic charts to show the data collected. It also allows you to measure satisfaction and collect feedback as you collaborate through the N365 platform either in SharePoint, on a Teams site/channel or in a meeting.

Access to Microsoft Forms is granted to all, however guidance must be followed as referenced on the N365 support site, and N365 procedure documents.

Any data you collect via Microsoft Forms **must be** registered on the Trust's Information Asset Register. You **must** familiarise yourself with the Information Asset guidance and policy to ensure compliance. You should also consider whether a DPIA is needed.

Child Protection & Safeguarding information pertaining to patients **must NOT** be held within Forms.

3.5 Microsoft Yammer

Microsoft Yammer gives users a central place to have conversations, create and edit documents and share information without sending emails or attending any meetings. With Yammer, employees will see posts in a newsfeed on their user engagement apps' dashboard whenever people update user info and they'll also be able to join in the conversation with their own posts.

Yammer has had little uptake/interest on the N365 platform and is currently not recommended for use by TSDFT staff, and therefore restricted. If access is required, please contact the Service Desk.

3.6 Microsoft Power Automate

Microsoft Power Automate allows users to automate manual repetitive tasks. Users can create automated workflows between a range of applications and services.

Power Automate doesn't store any data, it only holds configuration information. The data comes from the application(s) being used by the workflows such as Microsoft Excel, Outlook, OneNote etc.

Power Automate Developments currently require a managed approach that will be scoped and controlled within the N365 environment by the N365 Team. For further advice please contact the N365 Team via the Service Desk.

3.7 Microsoft Power Apps

Easily develop mobile and web apps for any business need—even if you have no technical or development experience—with Power Apps.

Power App Developments currently require a managed approach that will be scoped and controlled within the N365 environment by the N365 Team. For further advice please contact the N365 Team via the Service Desk.

3.8 Microsoft Whiteboard

Microsoft Whiteboard is a collaborative digital canvas in Microsoft 365 for effective online and hybrid meetings and engaging learning. All staff have access to this functionality, and data is securely stored in users' OneDrive.

4 Archiving & Retention

Under the ***General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA18),*** all personal data, including that stored as a message in Teams or in the NHSmail email system is subject to the GDPR/DPA18 data minimisation and storage limitation principles, which the organisation strictly adheres to.

All emails and archives messages, Teams, SharePoint, Streams, OneDrive and other N365 platform data are covered.

Full information on Archiving and Retention is detailed on the NHSmail support pages. Please refer to this for the latest policy guidance and procedures. Data Retention and Information Management Policy – Office 365 – NHSmail Support

5 Monitoring

The systems and software provided as part of N365 is licensed for employees use and as such will always be subject to being monitored. The organisation can access data stored on the platform as deemed appropriate.

- All NHS email is monitored for viruses, malware, phishing, and spam.
- All email (incoming and outgoing) on NHS systems is logged automatically.
- Monitoring logs are audited periodically.
- Activity Monitoring and Data Loss prevention tools are available to the organisation and will be used to ensure TSDFT's compliance with legislation and other obligations
- The personal and business use of email is not private. The content of email is not routinely monitored but the organisation reserves the right to access, read, print, or delete emails at any time.

- 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 Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 2018, the UK General Data Protection Regulation, the Human Rights Act 1998 and specific procedures around monitoring and privacy.

Data access is in compliance with our legal obligations; any data sent or received through the N365 system forms part of our business records and must be retained in accordance with our Retention Periods schedule.

6. Breaches of Policy

6.1 Investigation

The organisation will investigate breaches of this policy, actual or suspected, in accordance with the organisations HR & Disciplinary procedures.
Where appropriate, the organisation will make a complaint to an individual's employing organisation and co-operate fully into any investigation of that complaint where breaches of this policy are committed by users who are not employees of the organisation (such as staff on secondment, Honorary Contract holders and users given access to systems by agreement between this organisation and the user's employing organisation).

6.2 Outcomes of an Investigation

Where any employee has or is believed to have purposely breached the standards or requirements set out in this policy, or wilfully delayed reporting any incident they may face disciplinary action.
The disciplinary penalty will be proportionate to the level of misuse but can range from a verbal warning through to dismissal, dependant on the factors involved in the policy breach. Knowingly using N365 systems in a manner that does not comply with legal obligations, or this policy is a serious matter, and the organisation will monitor and review all use to ensure the correct procedures are being followed and adhered to.
The organisation will, where appropriate, take legal action (that is, criminal or civil proceedings) in respect of this policy.

7 Liability

The organisation will not be liable for any financial or material loss to an individual when using email or Office 365 for personal use or when using personal equipment to access work email.

8 Policy Review

This document may be reviewed at any time at the request of either staff side or management or in conjunction with any policy, legislation, or technology change. Otherwise, the expected review timescale for this policy is every 3 years.