Torbay and South Devon
NHS Foundation Trust

Document Type:	Procedure Guideline	
Reference Number : **SDHIS-N365-2**	Version Number: **1.1**	Next Review Date: **01-05-2025**
Title:	**Microsoft 365 Services Platform - Procedure**	
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 guidance 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-N365-2		
Document title:	Microsoft 365 Services Platform Usage		
Purpose of document:	Terms of usage		
Date of issue:	21-07-2022	**Next review date:**	01-08-2025
Version:	1.1	**Last review date:**	17-08-2022
Author:	Joe Taylor		
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 Policy – Microsoft 365 Services Platform		

Document Amendment History

Date	Version no.	Amendment summary	Ratified by:
13-09-2021	0.1	Draft	
17-09-2021	0.2	Internal N365 team review	
28-09-2021	0.3	Transferred into template from existing document. Formatting changes.	
19-10-2021	0.4	Changes by the N365 Project Manager prior to IM&T review	
19-01-2022	0.5	Changes by the N365 Project Manager	
11-05-2022	0.6	Changes to add recent additions to the platform	Phil Sweet
04-07-2022	0.7	Edits to reflect feedback received from HIS Director and IM&T Group per approval on 14th June 2022	Jai Ragwani & IM&T Group
21-07-2022	1.0	Publish following approval and minor spelling/grammar amendments.	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 Statement

Torbay and South Devon NHS Foundation Trust *(hereinafter referred to as the **"organisation"**)* 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 'On-prem' 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 Procedure should be read as an addition to our online support pages available here. Latest guidance will always be available online.
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 procedure 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 procedure is to provide staff with additional detail and guidance when using solutions within N365 and helps to reduce the risk associated with corporate use of the platform.

0.3 Scope

This procedure is applicable to all staff within the organisation *(meaning permanent, fixed term, and temporary staff, 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.

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

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

1 N365 Platform Guidelines

The N365 platform provides flexible and powerful systems and tools of great benefit to the organisation when used appropriately.

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.

1.12 Administrators

Administrators are typically members of the South Devon Health Informatics Service (SDHIS) and control overall access to the platform. They are required to:

- Manage user accounts alongside the **Workforce Information Team** (As part of the Joiners /Movers/Leavers processes).
- Manage guest accounts for people accessing the platform from approved external organisations.
  - **NOTE:** Guest accounts cannot be provided for members of the public as this is for organisation-to-organisation access.
- Setup and remove SharePoint and Teams Sites.

    - Owners must be added to these sites as they are set up and these will typically not be members of SDHIS.
- Allocate licenses to users as required.
- Provide support to the platform and escalate support to national teams as required.

1.13 Owners

Owners are required when a SharePoint Site, Teams Sites, or Private Teams Channel is set up. They are typically not members of SDHIS, but have some administration access and privileges such as the ability to:

- Add or remove members.
- Delete conversations.
- Change settings within the site/channel.
- Rename the group.
- Update the description or picture.

Owners have responsibility for:

- The veracity of information stored within the site they own.
- Controlling membership access and security permissions.
- Ensuring that access membership and security permissions are regularly reviewed.

Owners can be changed as needed over time.

1.14 Members

Members are regular users within your organisation who have been added to a SharePoint Site, Teams Sites, or Private Teams Channel 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.

1.15 Guests

A guest on the N365 shared tenant platform is anyone not using their NHSmail account (nhs.net) to access the platform. Guest access lets staff collaborate with experts, partners, vendors, suppliers, and consultants outside of the organisation. They can also be other NHS organisations that have not joined the shared tenant and are using dedicated O365 tenant platforms (typically their email address ends with '.nhs.uk').
More details concerning the Guest access process and capabilities can be found here:
https://support.nhs.net/knowledge-base/introduction-to-guest-access-process-and-capabilities/

1.2 Best Practice

The organisation suggests that when using the solutions within the platform that employees should adhere to the following:

- Minimise the use of Personal Identifiable Data**.** Definition: see Appendix A.
- The N365 platform must not be the sole storage location for any clinical data. It can be used as a collaboration tool, but never as a replacement for functionality within the core clinical system.
- The N365 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 on the appropriate clinical system.
    - Where content on the platform forms part of a record, it is the responsibility of the user to ensure 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 N365 platform application into a record management system:
        - MS Teams chats
        - Email content. Including any data contained in an attachment
        - Information recorded / noted from a Teams voice and/or video meeting

1.3 Security Requirements

SDHIS are responsible for ensuring that the network and infrastructure is adequately protected from viruses and malware. However, employees and users can also help to avoid security issues. In order to reduce breaches of data protection and confidentiality requirements as well as to minimise cyber security risks, it is important to understand and comply with the responsibilities below.

Users of the N365 systems must NOT:

- Send or open any attachment that is not recognised, authorised or has come from an unknown source.
- Disable or change any of the security settings applied by default to the organisations system and network.
- Alter any of the security settings on the device being used to access the N365 systems.
- Disclose your login or password or attempt to access another user's email system.
- Leave systems open, unattended and unlocked when leaving a desk or the room.
- Automatically forward email or create workflows that can send data from their account to non-NHS email accounts. Examples of non-NHS email accounts include Hotmail, Yahoo, Gmail, and email services provided by internet service providers.

- Send confidential or sensitive information to non-NHS email accounts. Examples of non-NHS email accounts include Hotmail, Yahoo, Gmail, and email services provided by internet service providers.
- Share access links to files and folders in SharePoint Online and OneDrive with external users (Known as External sharing). Only use guest accounts or email to provide 3rd parties access to data. Sharing data during a Teams meeting is allowed as long as it complies with guidance contained under the Teams specific guidance in this document.
- Include any personal confidential data such as names and addresses in the subject line of any emails.

Users of the N365 systems MUST:

- Use encryption when emailing confidential information to **non @NHS.NET** email accounts by entering the text **[secure]** before the subject of the message of an email. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets aren't used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment. Only emails sent to other **nhs.net** recipients are automatically secured.
  - The guidance for recipient of encrypted emails sent from an NHSmail account can be found here: https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/Accessing+Encrypted+Emails+Guide.pdf .
  - All internal **@NHS.NET** email addresses are secure, but any other NHS email address is not considered secure, and encryption should be used when sending to these accounts.
  - A limited number of email addresses can be regarded as inherently secure and encrypted these include @*.gov.uk and @*.pnn.police.uk. The full list of secure and encrypted email addresses is available here https://support.nhs.net/article-categories/sharing-sensitive-information

- Be aware that "**Allow everyone in your company**" or "**Organisation wide**" settings will allow **everyone in the NHS** on the shared tenant to view the data. Setting permission to "**Public**" could provide direct access to the data from the internet and should not be used unless specifically approved by the organisation's Information Governance team.
  - It is essential that when staff create or manage data that could be in, but not limited to SharePoint, Teams, or Streams, that security is set as **"Private"** within the Privacy Settings section not **"Allow everyone in your organisation"**, **"Public"** or **"Organisation Wide"**.

- It is also important not to reuse a MS Teams meeting created for one purpose 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 "access key" to the meeting. Sharing this key allows anyone the recipient to access the meeting once they have it. If this is a recurring 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 so each meeting is isolated from the other.
- Be aware that all documents which are final or form corporate records should be stored in line with TSDFT IT policy. This may be in network drives/ folders or within SharePoint.
- Be aware that all data on the N365 platform may be subject to Subject Access Requests and potentially Freedom of Information requests. This includes but is not limited to emails, MS Teams conversations, SharePoint data, OneDrive data, etc…
- Regularly review and accept responsibility for delegate or shared access that is provided to other staff.
- Ensure that any personal computer or device that is used for work purposes must be installed with up to date, approved anti-virus software and encrypted if any data is to be stored locally on the device. (Advice about anti-virus software and encryption of your personal device can be obtained from the **Service Desk**).

1.4 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 the Microsoft 365 policy, and policies relating to equalities and anti-harassment. Data stored in the N365 platform can also be referenced and used as part of the on-going COVID-19 inquiry, and any future inquiries whether local or national.

- 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 personally).

- 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.

1.5 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, please log a Datix incident via ICON: https://icon.torbayandsouthdevon.nhs.uk/areas/incident-reporting/Pages/default.aspx. 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 or Cyber Security teams in such circumstances **as soon as possible.**
- Any instances of suspected fraud should be referred to the **Local Counter Fraud Specialist**.

1.6 Personally Owned Devices

The N365 platform is accessible from any device anywhere, however there are certain conditions that must be adhered to when accessing data from a personally owned device. This includes, but is not limited to, a personally owned laptop, desktop, mobile phone or tablet. Please refer to the organisation's *Bring Your Own Device (BYOD) Policy* for further information.

Personal devices used to access the platform ***should:***

- Be encrypted
- Be fully up to date with the latest versions of the operating system (Patched)
- Require authentication (i.e., 6 Digit PIN, Complex Password, Fingerprint, FaceID)
- Lock after a maximum 5 minutes of inactivity
- Not be Jailbroken/rooted
- Feature a manufacturer-supported Operating System (still receives security updates)

- Have anti-virus software (if appropriate) which is fully up to date
- Users should submit any personal devices being used to access the organisation systems to SDHIS for security software installation and checks as required.

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 Acceptable Use

Users must accept the NHSmail Acceptable Use Policy when they first sign into their NHS email account: Acceptable Use Policy - NHSmail Support.

In addition to the national AUP, the organisation has adopted the below set of acceptable use guidelines for employees to follow when using the organisation email:

- Employees must report any unusual or flagged email messages to the **Service Desk** immediately.
- The organisation email should only be used for legitimate business purposes.
- Employees should access their emails regularly and respond to messages in a timely manner.
- Employees should indicate when they will not be accessing their email using the ‘Out of Office’ function, listing an alternative contact where possible.
- Confidential or sensitive information, including information about patients/service users and staff, must be encrypted if it is sent by email to a non **@NHS.NET** address.
    - Encryption is enabled by entering the text [secure] before the subject of the message of an email. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets aren’t used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment. See Security Requirements for more information.

2.2 Prohibited Use

In addition to the acceptable use and policies set out nationally and as outlined above under the platform guidelines, the below actions and forms of use are unacceptable

The organisation email must <u>NOT</u> be used:

- As the only method of communication if an urgent response is required.
- To sign-up to personal, inappropriate or non-business internet sites.
- For sending or forwarding *'chain letters'* or social content.
- To send unsolicited corporate, marketing or advertising material (spam) to large numbers of users unless it is directly relevant to the recipient's work.
    - This includes the broadcast of personal messages, advertisements or other non-business-related information via the organisation's e-mail systems.
- With external, web-based e-mail services (e.g., hotmail.com) for business communications and purposes.
- To automatically forward emails such as from out of office or other rules that can send data from their account to non-NHS email accounts. Examples of non-NHS email accounts include Hotmail, Yahoo, Gmail, and email services provided by internet service providers.
- To send confidential or sensitive information to non-NHS email accounts. Examples of non-NHS email accounts include Hotmail, Yahoo, Gmail, and email services provided by internet service providers.
- To send email messages from another member of staff's email account (other than with delegated access) or under a name other than their own. Staff can give delegated access (proxy access) to their account and give permission for colleagues or administrative support to send emails on their behalf.
- To send global emails to ALL staff and/or to ALL GP practices. There are processes that must be followed for such communications. Contact the Communications Team for advice.
- To send emails to large numbers of users unless the recipients have been blind copied (bcc).
    - If the email is not blind copied, individual email addresses will be visible to everyone on the list which may compromise a recipient's confidentiality.
- To send emails to a distribution list comprising members of the public unless the recipients have been blind copied (bcc).
- To use blind copying as a matter of course (except in the above circumstances) where its purpose is to withhold from the primary recipient the fact that an email has been copied to a third party. Communication should aim to be transparent and the use of blind copying in this manner an exception rather than the rule.

2.3 Best Practice

As email is used so often to communicate with other people, the organisation has set out email etiquette that should be followed by all employees or third parties using the organisation email. Emails should be treated with the same level of attention that is given to drafting and managing formal letters and memos. Appropriate use of the email system and message structure is essential to the organisation's reputation and for best practice when contacting customers or other entities. ***The organisation suggests that when using corporate email, employees should:***

- Word emails with care because voice inflections cannot be picked up and it can be difficult to interpret tone.
- Ensure that the **'to'** field is correctly populated before sending the email.
- Turn off **'Contact Auto-Fill'** for the recipient field so that the email system does not suggest the name of the person you are sending the email to.
- Not use the email system for sending personal employee content, discussions or opinions such as jokes, outside work events etc.
- Always ensure that the **'Subject'** line is populated with something meaningful and appropriate.
- Keep the email content brief and to the point - do not clog other employees email system up with lengthy emails if a meeting or phone call would serve better.
- Only use the **'flag'** or **'urgent'** options when the message is urgent or needs a time-sensitive response.
- Do not type in all 'CAPS' to get a message across or in the subject lines as in email terms it is seen as shouting and is not polite.
- Avoid putting confidential information in Calendar Appointments to avoid inadvertent breaches of confidentiality.
- Check when forwarding or replying to emails to ensure that you are not inadvertently sending personal confidential data, either within the email chain or its attachments
- Seek alternative confirmation of receipt when urgent information has been sent by email, either by reply email or by a follow up telephone call.
- Not include any personal confidential data such as names and addresses in the subject line of any emails.
- There are several security risks associated with communicating with patients by email. It is difficult to authenticate the identity of patients; communication between the organisation and patients who are using a personal email account or an account from a non-secure domain will not, without additional steps, be secure.
- Only communicate with patients on matters of a confidential nature if they can verify the identity of the patient and the patient is made aware that email is not a secure method of communication, and they consent and accept the risk. Services such as Complaints, who may have routine email contact with patients, should gain Information Governance approval for the process as a whole but not individual communications.
- Emails should be moved into the provided email archive solution when no longer needed short term, but the information still needs to be retained. This is to keep mailboxes as efficient as possible.

    - The standard user mailbox size on NHSmail is 4GB and it comes with a 100GB online email archive.
- It is the responsibility of all staff to delete emails they are 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.

2.4 Sending Large Attachments

Employees should avoid sending or forward large messages or attachments. 10MB should be regarded as the upper limit, but good practice is below 1-2MB. Many email systems will simply block emails larging than 10MB. The sending and storing of large attachments can adversely affect the TSDFT network. Be mindful of video and presentation files, as they can be significant in size.

- A large file transfer system is available centrally for all nhs.net email account users: https://support.nhs.net/knowledge-base/egress-large-file-transfer-web-form/

- Where the recipient is available via MS Teams, then that may also be used for transferring large files. Users should be aware that large files shared within a teams chat will also use up their allocated data storage quota within OneDrive.

2.5 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.

2.6 Spam and Phishing Emails, Messages and Calls

- Staff must be aware of and avoid opening unwanted unsolicited emails and messages known as Spam or Phishing.
- Some unsolicited messages contain malicious web links which are intended to compromise network security and / or steal confidential information by masquerading as legitimate communications. These are known as Phishing.
- Where such emails have be opened inadvertently staff MUST NOT click on any links within the emails.
- Such emails can be forwarded **as an attachment only** to spamreports@nhs.net.

- Where a link in has been clicked in a suspected phishing or spam email, the IT Service Desk must be informed immediately.
- The *Cyber Security Guide* available on the NHSmail website https://portal.nhs.net/Help/policyandguidance contains further advice and guidance on dealing with threats via email.

3. Microsoft Teams Use and Guidelines

Microsoft Teams is a collaboration hub of multiple Teams sites that combines voice and video conferencing with 'instant messaging' 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.

Teams Channels can be created under Teams to support dedicated discussion topics / expertise. There are two types of Channels:

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

The organisation has set out guidance for employees on how to use Microsoft Teams for best practice, acceptable use and any actions deemed unacceptable when using or accessing the organisation email.

3.1 Acceptable Use

Microsoft Teams and its associated applications are covered in the **NHSmail Acceptable Use Policy (AUP).**

In addition to the conditions laid out in the national AUP, the organisation has adopted the below set of acceptable use guidelines for employees to follow when using the Microsoft Teams solution:

- The organisation Teams communications should only be used for legitimate business use.
- It is essential that when staff create or manage an MS Teams site, that it's set as "Private" within the Privacy Settings section not "Allow everyone in your company", "Public" or "Organisation Wide". Failing to do so will make it available across the whole NHS, with all the information stored in the Team accessible to all.
- MS Teams is a secure system which can be used to share sensitive personal information. Before doing so please discuss with your line manager or seek IG advice.

- Please show with respect and consideration for your colleagues in any messages sent using MS Teams.
- Team Site and Private Channel owners are responsible for the veracity of information stored within it, controlling membership access and that access membership is regularly reviewed.
- Ensure that where the creation of a team is necessary, that a duplicate team does not already exist and that a channel within an existing team is not suitable for the intended purpose.
- The availability of any Teams Application on the platform does not constitute authorisation to use it within the organisation. Users are responsible for ensuring apps are approved for Trust use before using them. Please consult the Service Desk for clarification if required.

3.2 Prohibited Use

In addition to the acceptable use and policies set out nationally and as outlined above under the platform guidelines, the below actions and forms of use are unacceptable.

Microsoft Teams must NOT be used:

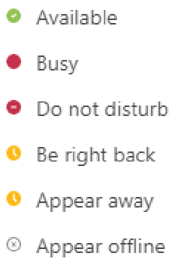
- For sending confidential messages to any unauthorised person or organisation.
- For sharing of organisation confidential data to external organisations/people.
  - To send, receive or access any copyrighted information in a way that violates or breaches that copyright.
  - In a way that could be expected to introduce any form of computer virus or malware into the organisation network.

3.3 Best Practice

Communication with others using Microsoft 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 of staff.

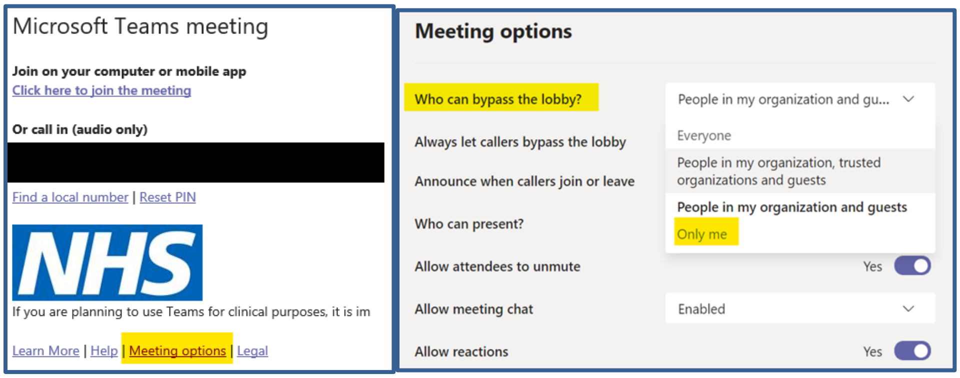
The organisation suggests that when using Microsoft Teams, employees should:

- Take note of other users' status updates as a common courtesy and to ensure effective communication *(see below for status options).*



● Available
● Busy
● Do not disturb
● Be right back
● Appear away
⊗ Appear offline

- Ensure Teams meeting recipients are BCC'd in if you wish to their hide contact details.
- Ensure that participants are included as **"required attendees"** in the meeting invite (especially for meeting invites generated from shared mailboxes) to ensure they are able to access the chat/recording/files after the meeting.
- Personal Identifiable Data **can** be safely verbally disclosed during video and voice conferences, but PID ***should <u>NOT</u> be openly used if the Teams meeting <u>is being recorded.</u>***
- 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 and made available through MS Teams may remain available indefinitely, depending on how individuals are included in any meeting or chat.
- Be aware that 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 OneDrive account for the person sharing the file.
- It is also important that a MS 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 anyone the 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 required 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 MS 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:
    - In the Teams meeting invitation, select the Meeting Options web link. Then adjust the "Who can bypass the lobby" option to "Only Me" as well as any other meeting security options.



Microsoft Teams meeting

Join on your computer or mobile app
Click here to join the meeting

Or call in (audio only)
[redacted]
Find a local number | Reset PIN

NHS

If you are planning to use Teams for clinical purposes, it is im

Learn More | Help | Meeting options | Legal

Meeting options

Who can bypass the lobby?	People in my organization and gu...
Always let callers bypass the lobby	Everyone
	People in my organization, trusted organizations and guests
Announce when callers join or leave	People in my organization and guests
Who can present?	Only me
Allow attendees to unmute	Yes
Allow meeting chat	Enabled
Allow reactions	Yes

- Teams is not currently suitable for direct patient video consultations where the patient is logging in or controlling one end of the call. ‘Virtual Visits’ within the N365 platform is specifically designed for patient consultations, however TSDFT currently use Attend Anywhere in line with other NHS Trusts in the South West.
- Use of MS Teams chat is mostly for brief and interactive communications, formal communications may still require an email.
- Be aware if you set up a Teams meeting in the Teams application rather than Outlook, then you can add a Teams Channel to the meeting. If you do this, 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.
- It is the responsibility of all staff to remove Teams 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 Teams Owners

Each Team site or private Teams Channel has Owners and Members. Owners have enhanced administration access, privileges, and responsibilities, whereas Members are consumers of Team Site functions. The following recommendations are for Teams site Owners:

1. Remove the ability for site members to create and update channels from the site:
   - Go to the Team Site and click ··· > **Manage Team**. On the **Settings** tab, expand **Member permissions** > untick:
     - **Allow members to create and update channels**
     - **Allow members to delete and restore channels**

     NOTE: This also removes the ability for both Guest and standard users
2. Review access to Teams Sites and private channels:

    - Go to the Team Site or private channel and click ··· > **Manage Team/Channel**. On the **Members** tab, expand **Member and guests** > Click the cross to remove members or guests as appropriate:

3. Ensure that only team owners can post to the General Channel:
    - Go to the General Channel team and click ··· > **Manage Channel**. On the **Channel Settings** tab, select **Only owners can post messages**.

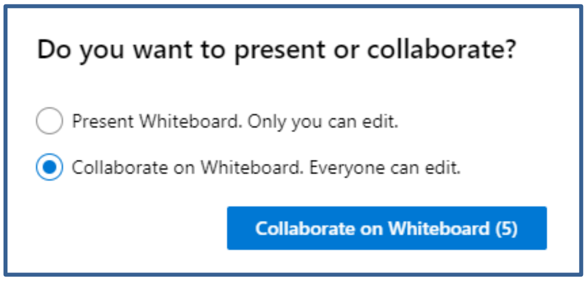
3.5 Screen Sharing Use and Guidelines

Microsoft Teams provides the ability for any user to share their screen, presentation or application as part of a meeting either scheduled or impromptu. It is very important to be aware of what you are going potentially present when sharing content in a meeting.

- Sharing a screen will show everything on that screen to all meeting participants. If you switch to another app on the shared screen, its contents will be also displayed to the participants.
    - Consider sharing an application or a specific presentation instead.
    - If you have more than one screen available, you may want to move the content and apps whose content you want to present to a screen you plan to share and move the other apps to another monitor. This saves you from extra adjustments and accidents during the meeting.
- Ensure you are prepared in advance.
    - Take a few minutes before your 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.
- Ask if everyone can see the content you are sharing.
    - Hold down CTRL on your keyboard and use the mouse scroll wheel to zoom in or out so elements more comfortable to view by participants.
- When presenting PowerPoint content, all meeting participants can browse the presentation slides independently. You can block this using the eye icon at the bottom left of the presentation. This is in the same place you will also find the browse buttons and the end presentation button.
- When presenting a web browser, separate browser tabs you plan to present on separate browser window to prevent accidentally sharing unwanted content to the meeting.

3.6 Microsoft Whiteboard Use and Guidelines

You can find Microsoft Whiteboard in the meeting sharing toolbar whilst a meeting is in progress *(via Share Content)*. As soon as the Whiteboard canvas has been started, you can then choose whether you wish other to collaborate or not.



Do you want to present or collaborate?

○ Present Whiteboard. Only you can edit.

● Collaborate on Whiteboard. Everyone can edit.

If you select the bottom option, Teams meeting attendees can ink and type collaboratively. To add ink, click the Pen icon, select a colour and then begin to draw, sketch, or write on the board. To add text, click the Note or Text icons, and then begin to type. Objects can be moved around on the canvas.

For richer functionality, Teams meeting attendees can open the whiteboard they're editing in the full-featured Microsoft Whiteboard apps for Windows 10 or iOS to add other content types and use additional features. These changes will appear in the whiteboard being edited in the Teams meeting.

Currently, a few pens, rubber and move functionality can be found on the Whiteboard of the meeting. You can draw on the Whiteboard with either a mouse or a stylus. To use the advanced features of Microsoft Whiteboard, open the application from Windows, create a new Whiteboard, and share it as an application to the meeting.

If you share a whiteboard during a Teams meeting that is being recorded, it will not be part of the recording. After a Teams meeting, its whiteboard will be available to all participants from the Teams meeting chat, in a tab labelled Whiteboard. The whiteboard will also be available in the Board Gallery in the Microsoft Whiteboard apps for Windows 10 and iOS, so that meeting attendees can continue collaborating on a whiteboard even after a meeting has ended.
Teams meeting attendees within the same Microsoft 365 tenant can collaborate on a whiteboard. Anonymous, federated, or external users are not yet supported.
In addition to the conditions laid out in the national AUP, the organisation has adopted the below set of acceptable use guidelines for employees to follow when using Microsoft Whiteboard:

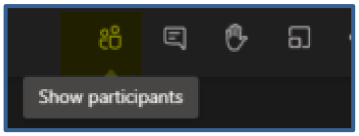
- Whiteboards should only be used for legitimate business use.
- Personal Identifiable Data should be avoided, but if necessary to identify a patient, this information should be anonymised.
- The **Collaborate on Whiteboard** can be used if you need input from other meeting attendees.
- Whiteboard must **NOT** be used for storing sensitive information including, but not limited to, passwords, pin numbers, door codes etc.

3.7 Video Calls and Video Conferencing Use and Guidelines

MS Teams and other video conferencing solutions are now in common use across the NHS and its partners. Whilst organisation expects them to operate standards similar to actual physical meetings, some additional considerations do exist.

- The participants should be aware who is present in a meeting and act in an appropriate manner.
- Staff should endeavour to attend meetings promptly and also avoid running over.
- Participant microphones should be initially muted especially on “busy” calls.
- Staff must try to avoid being overheard in an open-plan office / busy room in the house by having calls in a private room, particularly when confidential information is being discussed.
- Staff are encouraged to switch on cameras during video calls 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.
- For all calls between colleagues and partners, it is good practice and common courtesy to ask if anyone objects to the recording of a call. This provides an opportunity for objections to 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.
    - By Default, the recording permissions are set so only those invited to the meeting can access the recording in OneDrive or as a download. These permissions can be changed but remember that if security is changed to “Allow everyone in your organisation” or “Organisation Wide”, that permission is given to view from all NHS Organisations or the wider public.
- 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 we hold.
- Use background blur or a background image as appropriate. Especially if in a sensitive area where the background should not be visible.
    - Obscene or offensive backgrounds, whether real or virtual, are prohibited. Where an external participant has such a background, the meeting co-ordinator should take appropriate steps to remedy the situation or terminate the call.
- Do not use other applications or settings that filter or change your appearance.
- Where patients (or their representatives) wish to record a meeting using their own equipment, then staff should as a matter of routine facilitate this where it is for the patient’s own personal use. Covert recording by patients of their meetings may be regarded as impolite, it is not however prohibited.

- When someone other than the presenter wishes to speak, they should click the **raise hand** icon (under ‘reactions’) 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 participants tab.



- Consider the use of Live Captions. If anybody in your 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.
    - Each participant using a Teams desktop or mobile app can turn on live captions for themselves, but it’s currently **not available in the web interface**. To turn on live captions, move the cursor to summon the meeting controls toolbar, click the three-dot icon to open the “More actions” menu, and select *Turn on live captions*.

3.8 SharePoint Use and Guidelines

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

3.8.1 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.
- It is essential that when staff create or manage a SharePoint site, that it’s set as “Private” within the Privacy Settings section not “Allow everyone in your company”, “Public” or “Organisation Wide”. Failing to do so will make it available across the whole NHS, with all the information stored in the site accessible to all.
- 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.

3.8.2 Prohibited Use

In addition to the acceptable use and policies set out nationally and as outlined above under the platform guidelines, the below actions and forms of use are unacceptable and must not be used by any employees.

Microsoft SharePoint must NOT be used:

- As a sole repository for PID. It is imperative that all Personal Identifiable Data is retained in the appropriate clinical system/records management system, in accordance with our Retention Periods schedule.
- To download/copy content to a personally owned device. Files can be accessed and viewed/edited on personal devices but must not be stored on the device.

3.8.3 Best Practice

The organisation suggests that when using Microsoft SharePoint, employees should:

- Always be mindful that this is an internet connected applications 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.

3.9 OneDrive Use and Guidelines

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.

A standard user will be provided a OneDrive storage limit of 2GB. Additional storage can be procured if justified, via additional licensing.

3.9.1 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.

3.9.2 Prohibited Use

In addition to the acceptable use and policies set out nationally and as outlined above under the platform guidelines, the below actions and forms of use are unacceptable.

OneDrive must NOT be used:

- As a sole repository for PID. It is imperative that all Personal Identifiable Data is retained in the appropriate clinical system/records management system, in accordance with our Retention Periods schedule.
- To download/copy content to a personally owned device. Files can be accessed and viewed/edited on personal devices but must not be stored on the device.

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

3.9.3 Best Practice

The organisation has set out guidance that should be followed by all employees or third parties using OneDrive. Appropriate use of the OneDrive system is essential to the organisation's reputation and for best practice when contacting customers or other entities.
The organisation suggests that when using OneDrive, employees should:

- Use SharePoint or Teams for sharing files with others. It is easier to keep track of who has had files shared with them and ensure that confidential information is managed appropriately.
- Ensure that when leaving a post that all appropriate OneDrive data is transferred to an appropriate colleague or their manager, as agreed with their line manager or head of department.
- Use OneDrive when you need to store documents and/or other data on the device provided to you by your organisation.
  - Data stored locally (e.g., C: drive) on a desktop computer, laptop, or mobile device is not backed up and may be irretrievably lost if the device fails or is stolen.
  - Documents saved to Microsoft OneDrive on your organisation's device are synchronized with the cloud service when there is an internet connection, so it is

secure and retained under national policies. Information stored on OneDrive on your organisation's device is encrypted, both in transit and at rest.

If an employee leaves the organisation, it is the responsibility of that employee to ensure that their OneDrive data is transferred to an appropriate colleague or manager. The organisation may delete the data contained in a user's OneDrive account, before an employee leaves the organisation.

3.10 Microsoft Stream Use and Guidelines

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 Stream solution should only be used for legitimate business use.
- It is essential that when staff create or manage a Stream, that it is set as "Private" within the Privacy Settings section not "Allow everyone in your company", "Public" or "Organisation Wide". Failing to do so will make it available across the whole NHS, with all the information stored in the site accessible to all.
- 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.

3.11 Microsoft Forms Use and Guidelines

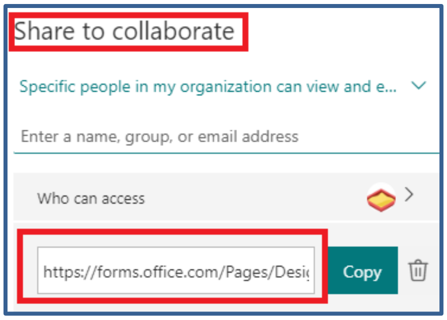
Microsoft Forms provides the ability for staff to create surveys, quizzes, polls and questionnaires, then make real time automatic charts to show the data collected. It also allows you to measure satisfaction and collect feedback as you collaborate through the N365 platform either in SharePoint, on a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

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 Forms solution:

- Clusters of information held in Forms must be registered as Information Assets. **What does this mean for you?:** any data you collect via Forms **must be** registered on the Trust's

Information Asset Register, the same as you would register any other data store. You **must** familiarise yourself with the Information Asset guidance and policy to ensure compliance. You should also consider whether a DPIA is needed.

- Forms that are used by a department (not by an individual) **OR** contain sensitive data must be held within a Team so that there is not a single point of failure and the data is still available should the user leave the organisation.
- Ensure questions are appropriate and have simple answers. Consider pre-populating answers with multiple choice, ratings or yes/no/maybe responses to get precise analytics.
- Microsoft Forms should only be used for legitimate business use.
- Forms created should include a statement of intent - why the data is being collected and what will be done with it.
- All individuals identified as collaborators must have a need to access this data as part of their role.
- It is essential that when staff create or manage a Form's security, that permissions are set to either **"Only people in my organization can respond"** or **"Specific people in my organization can respond"**. Permissions should not be set to **"Anyone can respond"** as this will make the form available across the whole NHS, with all the information stored in the site accessible to all.
- **Share to collaborate** links to forms must not be used where PID is being collected, as these links are not user specific and could be forwarded to an unauthorised user.


Share to collaborate

Specific people in my organization can view and e...

Enter a name, group, or email address

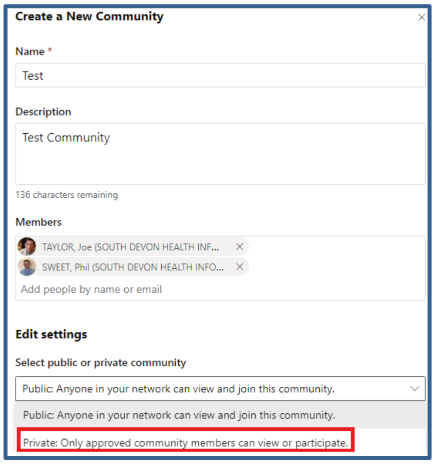
- It is the responsibility of all staff to remove Forms data they control when it is no longer required, in compliance with the organisation's wider data retention policies.
    - It is imperative that all data containing Personal Identifiable Data is retained in the appropriate records management system in accordance with our Retention Periods schedule.
- Child Protection & Safeguarding information pertaining to patients **must <u>NOT</u>** be held within Forms.

3.12 Microsoft Yammer Use and Guidelines

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.

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 Yammer solution:

- Before using Yammer, it is essential to be familiar with the Trust's Social Media Policy as regards acceptable use and duties & responsibilities: https://icon.torbayandsouthdevon.nhs.uk/corp_doc_mgmt/Clinical%20Effectiveness/Social%20Media%20Policy.pdf
- No offensive images should be uploaded to Yammer either as a new post or in the comments of an existing post. Please pay particular attention to the Prohibited Use section at the top of this document.
- The Microsoft Yammer solution should only be used for legitimate business use.
- Microsoft Yammer is not suitable for the sharing of Personal Identifiable Data and should not be used for this purpose at **ANY** time.
- When creating a Yammer Community, then this **MUST** be set to Private. If left as Public (the default option), then all posts will be visible to everyone on the shared tenant.



Create a New Community

Name *

Test

Description

Test Community

136 characters remaining

Members

TAYLOR, Joe (SOUTH DEVON HEALTH INF...

SWEET, Phil (SOUTH DEVON HEALTH INFO...

Add people by name or email

Edit settings

Select public or private community

Public: Anyone in your network can view and join this community.

Public: Anyone in your network can view and join this community.

Private: Only approved community members can view or participate.

- It is essential that when staff create or edit a Yammer post, that only relevant users are tagged in the post.
- If a Yammer post is shared, then it should only be shared to the relevant Teams Channel(s) and/or Yammer Community(s).

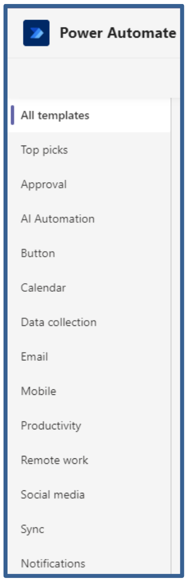
- It is the responsibility of all staff to remove Yammer posts they control when it is no longer required, in compliance with the organisation's wider data retention policies.
- Comments on posts should be related to that post only.

3.13 Microsoft Power Automate Use and Guidelines

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.

- An existing template should always be used where possible, if a suitable template exists. To find a template, use the categories down the left-hand side or use the **search templates** box.



.

- Power Automate should be used to create processes related to business use only.
- All requests for Power Automate should come in via an IT Project Request Form. Consideration can then be given for the work to be carried out by the local support team.
- Personally created solutions cannot be maintained or supported by SDHIS.
- It is strongly recommended that any users of the application familiarise themselves with the Power Automate blog and Power Automate Community, both located at the bottom of the home screen. Both are excellent sources of knowledge on how best to utilise this application.

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's/DPA18's 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 subject.

For emails, archives messages and OneDrive, staff data is stored for as long as 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 Office365 applications such as Teams, SharePoint, etc, data is stored until either the data is specifically deleted or the sites containing the data is 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.
As part of an official investigation, requests may need to be escalated to the national support team by an NHSmail LOA as per the following documentation:
https://comms-mat.s3-eu-west-1.amazonaws.com/Comms-Archive/Access+to+Data+Procedure.pdf
Information contained within the retention period of 180 days (since last edited) and live data can be accessed for the following Office 365 applications (when enabled):

- Corporate emails (including sent, received and archived messages)
- OneDrive
- SharePoint site collections
- Office 365 groups (including emails to groups, conversation, files transferred in Teams channels conversation and file transfers)
- Teams private (one-to-one) conversation (IM only)
- Recorded Teams conversations available via the application Stream
- Yammer

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 they deem appropriate.

- All NHS email is monitored for viruses, malware 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 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 Responsibilities

6.1 All Managers

All managers are responsible for:

- Ensuring that the staff they manage are aware of this procedure and their individual responsibility for complying with it.
- Ensuring their staff are equipped to fulfil their responsibilities as detailed in this document.
  - This will include covering it at their local induction and by identifying and meeting specific and generic training needs through personal development plans.
- Ensuring that email and OneDrive data is removed/moved as appropriate or closed down as required when staff leave the organisation, and that HR & IT are both simultaneously notified in good time so other elements of the leaver process can be completed in good time.
- Identifying staff who have been assigned wider administrative rights, have access to confidential/sensitive information or intend to use the solution on a personal device. These staff are recommended to use multi-factor authentication and report the requirement to SDHIS so their account can be upgraded.

6.2 Teams & SharePoint Owners

Any staff who have been set up as an 'Owner' of a Team Site, Private Teams Channel or a SharePoint Site are responsible for the veracity of information stored within it, controlling membership and guest access, and that access permissions are regularly reviewed.

6.3 All N365 Platform Users

All N365 users within the organisation are responsible for adhering to this document, the Microsoft 365 policy and for the correct and proper use of data on the platforms and ensuring the security of the information sent and received.

6.4 All Staff

All staff are responsible for reading and understanding the contents of this procedure document. Any questions are to be raised with their line manager for clarification or escalation as appropriate. They are responsible for reporting information incidents and near misses, including breaches of this policy as soon as possible so appropriate action to rectify such incidents can be taken to minimise any potential negative consequences. (See Reporting Incidents)

Staff who have been assigned wider administrative rights, have access to confidential/sensitive information or intend to use the solution on a personal device should notify SDHIS so they can enhance the security on the account by enabling two-factor authentication.

It is the responsibility of all staff to remove 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.

7 Appendix

7.1 Personal Identifiable Data

Definitions

Personal Identifiable Data is legally defined in the EU General Data Protection Regulation and the UK Data Protection Act 2018, The two together form the basis for our Data Protection legislation (DPL).

Under the DPL there are two distinct areas that are defined as Personal Data and as Sensitive Personal Data. Both make up that which is defined as Personal Identifiable Data.

Personal Data is classed as any information relating to an identified or identifiable natural person. This is supported by detailed by reference to a series of identifiers including name, online identifiers (such as an IP address) and location data.

Sensitive Personal Data: The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation*

These are also referred to as ‘special category data’.

Both Personal Data and Sensitive Personal Data are components of PID. Other areas that are reflected are the NHS Common Law Code of Confidentiality and the Caldicott Principles
Links covering the above can be found here:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/
https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/confidential-patient-information
https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx