# Microsoft Teams Acceptable use – Mersey Care NHS Foundation Trust

| | |
|---|---|
| Document Number | **V1.0** |
| Release | 16 September 2020 |
| Author | **IM&T Security Manager** |
| Owner | **Informatics Merseyside** |

## Revision History

| Revision Date | Brief Summary of Changes | Changes Marked |
|---|---|---|
| 16/09/2020 | | No |

## Approvals

This document requires the following approvals. Signed approval forms are filed in the project files.

| Name | Signature | Title | Date of Issue | Version |
|---|---|---|---|---|
| Jeanie Hedley/Laura Bow | J. Hedley | Information Governance | 30/09/2020 | V1.0 |

All staff using Microsoft Teams on the Office 365 tenant must observe the following:

- Users of Microsoft Teams must adhere to this document and the Acceptable use **Security Standard.**
- Teams created for Trust / CCG purposes should be deleted by the owner when the related project or program has been completed.
- Inactive Teams will be automatically deleted after 6 months of inactivity and *completely unrecoverable* from the recycle bin after another 30 days following their deletion. At that time, all data contained within the Team will be lost and cannot be recovered by Informatics Merseyside or Microsoft.
- Any documents shared via Teams that need to be kept after the project has ended must be saved in the relevant shared folder on the Trust's servers. Documents must be held according to the Trust's record retention periods (see the records policies for further guidance).
- All Teams created by staff should use a name that clearly identifies the use or purpose of the Team and must not include any inappropriate, offensive or hateful words, or any 'code' words that represent these things.
- MS Teams sites are provided for use in relation to Trust / CCG activity to support discussions, projects, collaboration and communication.
- MS Teams sites are provided to include members selected from across the organisation and external organisations. When creating Teams for use with external organisations, the group must be marked as Public.
- MS Teams is an Office 365 cloud service and therefore information contained within Trust / CCG sites is stored in Microsoft Data Centres. This meets UK and EU data protection and security standards.
- Interaction is encouraged. Chat-based collaboration is a useful tool when there is regular interaction and works best when there are multiple voices represented within the dialogue.
- It is important that staff recognise that this is a Trust / CCG provisioned service and therefore users must adhere to the guidance below or risk disciplinary action. Usage may therefore differ to the way you engage within external collaborative or social media sites designed for personal use.

## When using Microsoft Teams all staff must:

**Be transparent** – use your own name and photograph within your Office 365 profile. It is important that members are clear about who they are interacting with.

**Be safe** – MS Teams is designed to support secure networks, therefore, do not over disclose personal information and protect yourself against identity theft.

**You Must be aware** – That if Personal Identifiable Information is to be shared in a Team the Team owner is responsible for managing the members of that Team. Safeguarding all the data, you share.

**Only post to appropriate members** – all MS Teams channels and discussions are visible to all members of the MS Team site. Private messaging is available to send direct messages to selected members.

**Be professional** – be polite, don't not make or hijacking posts. Treat team members with respect. It is important that this is maintained throughout and even in instances when opinions differ. Be clear and avoid using ambiguous language which may be open to misinterpretation.

**Keep it relevant** – make sure you clearly understand the purpose of your MS Teams site. Stay on topic and avoid sharing irrelevant content as this may frustrate other members. No spam.

**Safeguard all data** – MS Teams provides a file storage location for files posted within conversations and channels. This provides a time limited repository and should not be used as a substitute for personal storage solutions such as OneDrive; staff personal Drives or departmental files storage. The Trust / CCG and Microsoft cannot guarantee that we can retrieve data previously saved in this location after the MS Team site is closed.

**Be aware** – when Sharing images and videos – you should ensure that the sharing of images and videos does not breach image rights and copyrights. Seek permission from anyone included in personal photographs prior to sharing them.

**Be Alert** when Sharing confidential, personal and sensitive information – in most instances there is no need to share Confidential or Personal or Sensitive information via MS Teams and this should be discouraged within the MS Teams site. Individuals Personal and Personal Sensitive information must not be requested or shared. Where there is a need to share Confidential information this should be labelled as 'Confidential'; appropriate permissions should have been sought from the data owner prior to sharing; the purpose of sharing the data should be transparent to the group and there should be a clear timeframe set to ensure that this data is removed as soon as it is no longer needed. The sharing of Confidential, Personal and Sensitive information increases the risk of data breaches and when breaches occur this may result in disciplinary action taken against the individual sharing the data.

**Not Share** – information outside of your private teams – information shared within your private Team is for use by the Team members only and should not be shared outside without appropriate permissions. No Confidential, Personal or Sensitive information should be shared outside of your private Teams.

**Use appropriate posts** – the Trust / CCG reserves the right to remove inappropriate MS Teams sites or posts. This may include posts that damage the reputation of individuals or

the organisation, including defamatory comments that may cause distress to members of our Trust / CCG, that contain obscene content or breach civil or criminal law. If you post inappropriately and later remove this post this may still be accessed by the Trust / CCG and used within disciplinary procedures as appropriate. Typically, a MS Teams site will have two nominated site owners who will monitor use and ensure inappropriate posts are removed. Such posts may lead to disciplinary action

## Teams Recordings

All Teams recordings are stored in Microsoft Stream within Office 365 Storage.
The organiser of the meeting and the person who started the recording will be able to edit the recording. Everyone invited to the meeting will also be able to view the recording.

Due to the possible sensitivity and confidentiality of some Teams meetings, the recording feature is **disabled** by default.

**If this** feature is required, it can be requested via the service desk and approval will be required from your service director.

## Glossary of Terms

**Teams** are a collection of people, content, and tools surrounding different projects and outcomes within an organization.

- Teams can be created to be private to only invited users.
- Teams can also be created to be public and open and anyone within the organization can join (up to 10,000 members).

A team is designed to bring together a group of people who work closely to get things done. Teams can be dynamic for project-based work (for example, launching a product, creating a digital war room), as well as ongoing, to reflect the internal structure of your organization (for example, departments and office locations). Conversations, files and notes across team channels are only visible to members of the team.

**Channels** are dedicated sections within a team to keep conversations organized by specific topics, projects, disciplines—-whatever works for your team! Files that you share in a channel (on the Files tab) are stored in SharePoint. To learn more, read How SharePoint Online and OneDrive for Business interact with Teams.

- Channels are places where conversations happen and where the work actually gets done. Channels can be open to all team members or, if you need a more select audience, they can be private. Standard channels are for conversations that everyone in a team can participate in and private channels limit communication to a subset of people in a team.
- Channels are most valuable when extended with apps that include tabs, connectors, and bots that increase their value to the members of the team.

- **SPAM** irrelevant or unsolicited messages, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

## Appendix 1

Acceptable Use Security Standard