NHS
Liverpool
Clinical Commissioning Group

NHS Liverpool Clinical Commissioning Group
Information Governance

MS Teams Acceptable Use Policy

Documentation Control:

Version	Version V0.1
Ratified by	
Date Ratified	
Author(s)	John Webb
Responsible Committee/Officers	SIRO
Date Issue	29-September-2020
Review Date	29-September-2021
Intended Audience	All CCG Staff

Further Information about this document:

Name	MS Teams Acceptable Use Policy
Contacts(s) for further information about this document	John Webb
This document should be read in conjunction with	LCCG IG policies
Published by	NHS Liverpool CCG
Copies of this document are available from	LCCG Intranet - IG Policy section

Version Control:

Version Number	Reason/Group	By	Date
0.1	New guidance to support roll-out of Microsoft Teams across the organisation	JSW	29/09/20
1.0	Changes following IG Steering Group review	JSW	29/09/20

Table of Contents

1. Purpose

The purpose of this document is to define acceptable standards of behaviour for any CCG Users of MS Teams.

2. Scope

It applies to all 'CCG Users'– comprising LCCG staff, Governing Body members, temporary or agency staff, contractors, volunteers, students and any other staff who use MS Teams functionality provided by Liverpool CCG.

3. Compliance with Policy

All CCG Users of MS Teams must adhere to this document and the CCG's IG and security policies and procedures. Failure to do so may result in disciplinary action.

4. Acceptable Use of MS Teams

All Liverpool CCG Users of Microsoft Teams must observe the following:

- Teams created for 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 be *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 CCG's record retention policies.

- 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 or abbreviations that represent these things.

- MS Teams sites are provided for use in relation to CCG activity to support discussions, projects, collaboration and communication.

- MS Teams sites can be provided to allow collaboration between members selected from across the organisation and members from external organisations. Extra care must be taken when creating Teams for use with external organisations to ensure the correct people are sent an invitation

with a security code is to join any private teams. If a site is created that is open for anyone to join, the group must be marked as Public.

- MS Teams is an Office 365 cloud service and therefore information contained within 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 Users recognise that this is a 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 Users 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, but do not over disclose personal information and always protect yourself against identity theft.

You Must be aware – That the Team owner is responsible for managing the members of that Team and Safeguarding all the data you share. This includes ensuring that any team members from external organisations are aware of and adhere to this acceptable use policy.

Only post to appropriate members – by default, 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, treat team members with respect, and don't make derogatory remarks or hijack other member's posts to discuss an unrelated topic. 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. Always remember that information in Teams may be disclosable under Freedom of Information requests, Subject Access requests, or disciplinary procedures.

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. Never post spam.

Safeguard all data – MS Teams provides a convenient 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 more permanent storage solutions such as OneDrive; staff personal Drives or departmental files storage. Data should be assumed to be irretrievable after an 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 information –An Individual's or patient's Personal and Personal Sensitive information must not be requested or shared on any CCG sites. Where there is a need to share Confidential organisational information within a Team, 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. Disciplinary action may be taken against any individual sharing Confidential, Personal or Personal Sensitive information inappropriately.

Do Not Share – information intended for your private teams with others. Assume that information shared within your private Team is for use by the Team members only and should not be shared outside without appropriate permissions.

Use appropriate posts – the 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, defamatory comments that may cause distress, or that contain obscene content or breach civil or criminal law. If you post inappropriately and later remove the post this may still be accessed by the 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. However, such posts may still lead to disciplinary action.

Be extra careful with your own devices – MS Teams is designed for ease of access from most types of device. Users should never access their CCG MS Teams account from an unknown/insecure device such a public-access PC or tablet. If a User chooses to access Teams from their own personal device, then they must shoulder certain responsibilities to keep this access secure. Users must:

- Ensure your device has reasonable security measures in place, such as a strong password/unlock code, automatic locking after a period of inactivity, plus an up-to-date operating system and anti-virus protection;
- Always manually enter your Teams username/password information each time; DO NOT save your password onto the device;
- Minimise the number of people with access to your device;
- Ensure you DO NOT leave yourself logged into Teams when other people may have access to the device.

5. 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 so that 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.

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