information
management & security

Gloucestershire
COUNTY COUNCIL

M365 Acceptable Usage Policy

This should be read in conjunction with the following:

- Code of Conduct for Employees
- ICT, Information Management and Data Protection Policies, in particular;
    - ICT Equipment Policy
    - Information Protection and Handling Policy
    - Information/IT Access Policy
    - Data Protection Policy
    - Software Management Policy
    - Social Media Policy
    - Password Policy

You are also bound by any relevant legislation, such as data protection and copyright laws and the information below.

Misuse of the services can be investigated and lead to disciplinary action. The council reserves the right to monitor use and compliance with the law and policy; we may use system analytics to achieve this.

1.0 Microsoft Teams

1.1 Policy Statement

Gloucestershire County Council (the council) accepts that use of Microsoft Teams is essential to enabling the council to meet its aims and objectives. It is a requirement that your use of this software is legal and appropriate for delivering the council's responsibilities does not create unnecessary risk.

Microsoft Teams enables you and your colleagues to send instant messages, make video calls and keep up to date with your teams. Over time we will be adding more functionality allowing you to better collaborate, share and edit files as a Team and with external partners where appropriate. For now, you should use Teams as you would Jabber and WebEx.

Because Teams allows for greater interaction between council employees, the council must ensure that it is used appropriately and responsibly. This usage policy sets out how to do this, makes staff aware of how Sites should be managed and how new Sites can be requested.

1.2 What can you use Teams for?

Currently you should use Teams for the following:

- Chat and call with Council colleagues,
- Use Teams to create meetings with council colleagues and partners from other organisations
- Create and host Teams Webinars

Once we have ensured that appropriate security and protections are in place staff will be able to use Teams to work more collaboratively internally and with third parties.

1.3 Best Practice

Below are some best practice guidance you should follow or be aware of.

Chats

- You should not create separate channels for private one-to-one chats or group chats. You can do this without creating new Teams Sites or Channels.
- Do not share sensitive information through the chat. Teams is not an appropriate way to share sensitive information about customers. We have implemented security policies to prevent this.
- If you are asking a colleague to check a certain record in a system, use reference numbers instead of names to minimise the risk to personal data.
- You can get a colleague’s attention by typing @ and their name into the chat, but please try to avoid them whilst they are in meetings so as not to disturb them.
- Check the presence status to see if someone is available before messaging them. If you message someone whilst they are showing as busy, offline, do not disturb, be right back or appear away you may not get a response.
- Any instant messages you receive while offline for under a week will be available next time you come online.
- Remember that all chat content, whether direct or within channels is searchable and therefore could be disclosable under HR, audit or legal investigations, FOI or subject access requests.

Meetings and calls

- Double check you have sent any meeting invites to the correct attendees.
- Follow our guidance on when and how to safely record meetings in Teams.
- Be careful not to enter information into the chat rather than discuss it in the meeting. Anyone invited to the meeting can see what is written in the chat, even if they do not attend.
- Do not use one meeting to meet with multiple guests, where they need to be met with individually. Guests to a meeting have full access to the chat that is created from the meeting, even after leaving.

Webinars in Teams

A webinar in Microsoft Teams is almost identical to a meeting, with some additional built-in functionality. Webinars are structured meetings where presenters and participants have clear roles. A key difference between webinars and Teams meetings is that webinars support registration and provide attendee engagement data.

A webinar is useful when you want to broadcast a session to a large audience and have structured Q&A or breakout sessions. A Teams meeting is more appropriate when you have a smaller audience or want to allow equal opportunity for contributions.

When using Teams Webinars you should follow these steps:

- Unless there is a good reason not to, leave attendees' microphone and video turned off. This will reduce distractions by unwanted attendee videos or audio, but also make sure that the recording doesn't contain any video that shouldn't be captured.
- You must only collect details from potential attendees on the webinar registration form that are necessary for the purpose of the webinar. By default, the system includes first name, surname and email on the form. You may also wish to capture the attendee's job title and the organisation they work for. If you are collecting more than this, you will need to be able to justify why to meet data protection requirements.
- Ensure you only admit those people who are entitled to be at that webinar. Only use 'admit all' if you are confident that everyone in the lobby should be admitted.
- If you will be discussing personal or other sensitive information in your webinar lock your webinar to prevent others from joining.
- Attendance and registration lists should not be routinely kept. Those that need to be kept as evidence, such as to prove staff attendance at a training event, need to be downloaded and saved in the relevant network folder or SharePoint library.

Guidance on setting up Webinars.

1.4 Roles and Responsibilities

There are two roles within M365 for a Team; Site Owners and Site Member. Most users of a Teams Site will be members. There are three types of site members;

- Site Member (internal)
- External Member – Someone from outside the council who has been invited to a specific meeting
- Guest – an External Member who has been given access to a Teams Site.

Within GCC we have an additional role, with a senior officer being allocated accountability for the information within each site – this is the Information Asset Owner (IAO) or Manager (IAM).

Site Owner (Accountability) – IAO

IAOs are accountable for ensuring that any of their information assets, or extracts from those assets, are managed appropriately within Microsoft Teams, in line with their responsibilities.

Site Owners (Administrative)

Site Owners are **responsible** for:

- Adding or removing members and guests when necessary.
- Creating and deleting Teams Channels when necessary and in accordance with the council's design principles.
- Ensuring there are sufficient active system owners for the specific Team site (a minimum of 3 per site).
- Ensuring that the use of information on the Teams site is compliant with this AUP and council policies.
- Ensuring that chats within Teams Channels are used in an appropriate manner and follow council policies on appropriate behaviour.

All staff (site members)

All staff are **responsible** for:

- Their own activity within Teams.
- Ensuring that the use of information on the Teams site is compliant with this AUP and council policies, and
- Ensuring that chats within Teams are used in an appropriate manner and follow council policies on appropriate behaviour.

Retention & Monitoring

- One-to-one and one-off group (e.g. non-Channel) chats are retained for 24 hours.
- Teams sites are retained for 6 months after last use. At that point the Site Owner will be contacted and asked whether there is any business need for the Teams site to be kept for longer. Otherwise, the Site will be deleted.
- Team channel chats are retained for 3 months after last use.
- Please note that the system may retain chats, channels and sites beyond the retention periods above, even if they are no longer accessible to you. These can also be used in e-discovery activity.

2.0 OneDrive Usage Policy

2.1 Policy Statement

OneDrive is your personal area within the M365 environment for storing information relating to you in a work context. This usage policy sets out how your OneDrive should be used, and describes the information management and security settings and requirements.

2.2 What can you use your OneDrive for?

By default only you have access to information in your OneDrive, therefore it is not an appropriate location for information you want to collaborate on or information your colleagues need access to in your absence. Your OneDrive should be used for:

- Personal information relating to you in a work context e.g. timesheets and communications with HR;
- Personal training and development documents;
- File notes for your reference only;
- Information required for your day-to-day work that is personal to you; and
- Corporate information that may be in a very early draft. When you need to start collaborating on the document it should be moved to a network drive or shared area in SharePoint when available.

Your OneDrive should **not** be used for:

- Corporate information required for your day-to-day work, that needs to be accessible to colleagues, this information should be stored in network drives or SharePoint when available to be accessible via Teams;
- Staff management information such as formal 1:1 notes and PDRs, this should be stored in the HR document storage system (OpenText) when available, more informal catch-up notes may be stored in the OneDrive;
- Information about service users, this should be in the relevant case management system, for example Liquid Logic;
- Information that demonstrates decisions or agreements made e.g., contracts; or
- Personal photos, music, or films.

2.3 Information Management and Security

OneDrive Size

Due to limited use cases of OneDrive (see What can you use your OneDrive for?) a quota limit of 1GB for storage is in place.

If you exceed the limit you will not be able to save any more documents to your OneDrive until space has been cleared by deleting documents or moving them to another location such as SharePoint/OpenText.

Sensitivity Labels

The default sensitivity label for OneDrive is Non-Business, this reflects the more personal or informal nature of the documents that should be stored in your OneDrive. However, Official sensitivity labels, including Official-Draft, will be available to staff to apply as necessary.

Sharing

By default, only you will have access to the documents stored within your OneDrive, however, you can share individual documents and folders with other users within GCC at your own discretion for working on early drafts or sharing something personal with HR, you can also remove users access from any files that you have shared. Remember when you need to collaborate on a document with colleagues then it should be moved to SharePoint.

You cannot share information from your OneDrive with individuals external to the organisation via links. To share information to colleagues external to Gloucestershire County Council, the document will either need to be sent as an attachment or moved to a more public SharePoint location.

E-Discovery

Information stored on the OneDrive is still part of GCC's corporate M365 network and is discoverable using the E-Discovery function and could be accessed and disclosed as part of a Freedom of Information or Subject Access request, HR, audit or legal investigation.

Retention and Monitoring

OneDrives will be deleted 30 days after the departure of the owning member of staff. Line managers should ensure that all corporate information is moved from OneDrive before the member of staff departs.

If there are concerns that there is corporate information stored on OneDrive after the departure of the user, in extenuating circumstances an extension to the 30 days may be applied. The line manager may request that a hold for a set period of time is placed on OneDrive and an eDiscovery search carried out to identify corporate information to be retrieved. To do this please contact the IMS team stating:

- The name of the user's account;
- The justification for the extension of 30 days; and
- An outline of the information believed to be stored on OneDrive

2.4 Roles and Responsibilities

As OneDrive is by default only accessible to the owning user all staff are responsible and accountable for:

- How they use OneDrive and all information stored within it, and
- Ensuring the use of information on your OneDrive is compliant with this AUP and GCC Policies.
- Ensuring that access to information is granted appropriately where sharing with colleagues.

3.0 Yammer Acceptable Usage Policy

Welcome to Yammer. Our goal is to provide a collaborative environment to connect colleagues and bridge our departments and geographic locations, helping to build collaboration and connections.

Yammer provides informal social networking and communication. It is suitable for discussions, but should not be used for managing projects and sharing working files. Long term we will have Teams and SharePoint which are much better for that type of activity.

Yammer will encourage an array of diverse communities (Yammer groups) that will uphold the council's values and provide spaces for fruitful contact and development. Where posts are experienced as unsuitable or offensive, or the service is being misused, the council will investigate. The council reserves the right to monitor use and compliance with the law and policy and may use system analytics to achieve this. Inappropriate use may lead to disciplinary action and removal of that Yammer group.

Information posted on Yammer is attributed to the individual and does not necessarily reflect the views and opinions of the council. Any official council announcements should be made through standard communication channels and not linked back to content stored on Yammer.

3.1 Your personal data

Be aware that this is a visible space within the council – your details are available to everyone in the council's Yammer community.

Only share what you are comfortable with other people knowing about you.
Yammer is hosted on the Office365 cloud service hosted in the EU and governed by EU data protection policies.

All posts, even posts you delete, are searchable, readable and potentially disclosable, such as in response to official requests for information and HR, audit or legal investigations. If you wouldn’t say something to someone’s face it should not be posted here.

3.2 Information management and security

Groups are a great way to get the right people together to discuss appropriate topics, please check that a similar group doesn’t already exist when requesting the creation of a new group.

Everything in Yammer should stay in Yammer (no public posts or tweets, and so on). Information posted on this site is for internal purposes only and must not be shared outside of the council without appropriate authorisation. Don’t screenshot/take photos of conversations and use them elsewhere, such as on other social media platforms or messaging services.

Make sure you protect other people’s privacy as well as your own. Don’t share personal details, whether this be yours or anyone else’s and don’t share content that you don’t have legal permission to use.

Official Sensitive, personal information about others or confidential information is not to be posted onto Yammer, even if in a private group.

Yammer isn't a record keeping system and shouldn't be used as such. As soon as postings on Yammer become something that needs to be formally recorded (e.g. discussion leading to a business decision or study notes you want to keep), then additional records must be created and stored outside of Yammer.

Don’t lose your data - we do not offer a data retrieval service for Yammer.

Make sure you have a strong password. Don’t share your password. Always lock your workstation before walking away.

3.3 House rules and etiquette

- You are responsible for what you write and post to Yammer. This is a work tool provided by your employer to improve the way you carry out your job. The comments you make here may be visible to many.
- Posts in the All Company main feed are managed centrally, but you can comment on posts. Be aware that everything you comment on in the main feed can be seen by all.
- Share and like good content.
- Add value with each post.
- It is important to substantiate ideas, but please keep messages brief and to the point.

- Be respectful to other members. It is acceptable to disagree, but please do so in a respectful manner. Be polite; try to be constructive; don’t be offensive.
- Be mindful of how your comments might be read by others; think about whether or not what you are posting is appropriate for the audience you are posting it to.
- Apologise quickly if something is misinterpreted or taken the wrong way.
- Keep it professional – in the same way that we moderate our conversations in the office, you should apply similar moderation to posts here.
- And finally, be sensible - no spamming, unrelated or inappropriate posts, and be nice - no haters, no trolling, no hijacking posts.

4.0 Document Control

4.1 Document information

Owner:	Jenny Grodzicka, Head of IMS
Author:	Nick Holland, Senior Information Governance Adviser, Ellie Burgess, Corporate and Digital Records Manager, Jenny Grodzicka, Head of IMS
Last Reviewer:	Zoe Vernon, Information Assurance Support Officer
Date created:	August 2022
Next review date:	November 2023
Approval:	As separate policies: Teams – Information Board, 13th July 2022 OneDrive – Information Board, 22nd March 2022 Yammer – Information Board, 11th November 2021
Version:	1.1
Classification:	UNCLASSIFIED

4.2 Version History

Version	Version date	Summary of Changes
1.0	August 2022	First version, combination of Teams, OneDrive and Yammer AUPs
1.1	November 2022	Accessibility review and updates to formatting. Approval information moved to document control section, broken links fixed.

4.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

4.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: dpo@gloucestershire.gov.uk
Phone: 01452 324000