Using Yammer securely

Government staff are responsible for checking the applications they use are secure. This guidance will help you use Yammer to communicate securely with colleagues.

Yammer is a cloud application for social networking within an organisation, or with partners, customers, or vendors. You can use it to post updates and send messages, either directly or in a group. You can also use it to share documents, join groups, and search history.

Yammer is available as a stand alone service but is more often used as part of Microsoft's Office 365 suite.

Securing your account

Secure your Yammer account by using:

- a password made up of 3 random words
- a secure (HTTPS) connection and a modern browser

in Office 365. Secure your Office 365 account using two-factor authentication. You cannot use two-factor authentication in a stand alone Yammer account.

If you think someone may have accessed your stand alone account:

- logout any other sessions in Settings - Account Activity
- reset your password in Settings - Password

You can also delete your Yammer account under Settings - Preferences - Delete Your Yammer account.

Protecting your data

To protect your data when using Yammer, make sure you:

- don't use standalone Yammer to store sensitive, personal, or other high value data (like commercial or financial information) that could cause harm or embarrassment if lost or exposed - speak to your security team about what you can store in Office 365
- create and use internal groups with private access, and private messages when you need to control access
- Yammer is restricted to your email domain by default but you can create external groups if appropriate

When using Yammer, you should also be aware that content, including archived or private content, can be:

- disclosed publicly under the Freedom of Information Act

- exported and viewed by administrators in paid Yammer accounts, including private messages and groups
- subject to legal requests to share data by courts, government agencies, or parties involved in litigation in the US

Using Yammer for social or personal use must:

- not create exposure to legal liability or embarrassment
- not affect your performance or disrupt others
- follow the Civil Service Code

Microsoft - who run Yammer - have signed up to the EU-US Privacy Shield which requires them to follow European data protection requirements for personal data for their European customers. You own the data you put in Yammer, and their technical security is similar to other popular public cloud services.

Managing information

You must record or summarise important work in a permanent record at regular intervals or at the end of a piece of work.

Make sure you don't lose content by:

- creating a permanent record of shared information at regular intervals or at the end of a piece of work
- using your document storage or email service to capture important discussions or decisions (name the data so it can be found later)

You can export data from Yammer by:

- copying and pasting the text (while noting the date)
- taking a screenshot
- asking your administrator for an export in paid accounts

Getting started

Ensure your account looks official and similar to other government Yammer accounts by:

- use a recognisable profile photo
- add your role to the Job title section

You can alert others to content you have shared on Yammer by typing @username (their email address without the @domain.gov.uk) and by including the organisation or group name when posting an update. all or @here. This can trigger notifications on their computer or phone. Admins can post an announcement that will trigger an email alert as well as a post.

Getting help

For help using Yammer, you can use their getting started guide.

Yammer and Microsoft offer support through a:

- support page
- status page

You may also get help from your internal IT team if they have agreed to do it.