Teams site Owner responsibilities

As a University of Manchester Teams site Owner you have the following responsibilities. These relate to the individual Teams and their underlying SharePoint sites (which together are referred to as a 'Teams site' in this document).

A. Notes

1. A new Teams site is set as Private by default. Private Teams can only be joined if a site Owner adds someone to them.

2. Each Teams site must have a minimum of two site Owners who must be members of staff at the University. There can be more than two site Owners and additional Owners can be added by the existing Owners.

3. A maximum of two site Owners are permitted to be able to invite Guests to a Teams site. If a site Owner will need to be able to invite Guests (as distinct from Members) to the Teams site, a request must be submitted as a "Microsoft Office 365 request" via the IT Services Support Portal for access to the Guest Inviter role.

B. General responsibilities

1. As Teams site Owners you are responsible for the management of the Teams site.

2. Members, including Guests, must act in accordance with your instructions and will consult you if unsure of their responsibilities.

3. In your management of the Teams site, you must adhere to data protection legislation, relevant data sharing agreements and contracts, and the University's policies and standard operating procedures, in particular:

    a. University Export Controls

    b. Acceptable Use of IT Facilities and Services – SOP for Staff

    c. Information Security Classification, Ownership and Secure Information Handling

    d. Document and Information Management

    e. Privacy guidance when recording meetings

4. You should familiarise yourself with the Privacy Notices related to the use of Guests' personal data and other personal data processed by the University: https://www.manchester.ac.uk/discover/privacy-information/data-protection/privacy-notices/

C. Managing information in the Teams site

1. Teams site Owners are the Information Store Owners for the site. Further information regarding the responsibilities of Information Store Owners can be found in the Information Governance Accountability and Assurance Framework.

2. Teams site Owners are responsible for structuring the site in a way that ensures the information is manageable, useable and protected. Some contracts impose requirements as to where information can be stored and how it must be protected. You must ensure that your Teams site and use of information is compliant with these requirements.

    - As an example, it may be necessary for there to be a contract in place before adding a Guest where controlled information may be involved.

In order to assist you in managing information in your Teams site, you may like to refer to Sharing and storing information | Information Governance Office | StaffNet | The University of Manchester

3. Periodically you may be asked to apply information security classifications, to validate that members and guests are still accurate, to check external sharing, and to consider retention and disposal actions.

D. Granting access to Members and Guest Members

A Teams site member is a person who has access to your Teams site. There are two types of members:

- 'Members' - internal users with University of Manchester IT accounts
- 'Guests' - external users who have a guest account in Microsoft 365 (their account is created the first time they are added to any Team)

Once they join a Teams site, Members and Guests may be able to see all chats, posts and files shared within the Teams channels to which they have access, including historic chats and information. This means there are risks which must be managed by you as the site Owners.

Personal information (e.g. information about research participants, students or staff) must not be shared with Guests unless there is a contract in place which permits this, including a data processing agreement. Providing access to Guests without this may be in breach of data protection legislation.

Before granting access

1. When considering giving a new Member or Guest access to the Teams site you should first clearly identify why the access is necessary.

2. Giving access to Guests creates additional levels of risk and there are some steps to take before you do so:

    a. If needed, request Guest Inviter permissions for up to two site Owners (see A3 above).

    b. Check on Export Control requirements (see section E below).

    c. Check for any additional data protection and contractual requirements relating to Guest access.

    d. Carefully check the identity and contact details of the proposed Guest and confirm the email address you have is accurate. Wherever possible, Guests should provide their business / organisational email address to register their access rather than a personal consumer email address (e.g. Gmail) as this helps to identify the organisations that have access to university data.

    e. An account is created for a Guest the first time they are added to a Teams site. Although this means that they will then appear in the search list and could be selected by an Owner for membership of additional Teams sites, the same due diligence must be performed when adding an existing Guest to a new Team as when inviting a Guest for the first time.

    f. Ensure that the Guest has received a link to the Terms of Use for Guest Users of University of Manchester Teams Sites and is aware of the key policies and procedures which apply to the use of Teams.

When granting access

1. You should be sure to add the correct person to your Teams site. Failure to do so could mean that unauthorised individuals gain access to the posts and files within the Teams.

2. The Search list which is provided in Teams to select new members may not contain sufficient information to enable accurate identification, so use their email address to search instead of their name.

3. University staff must only use their university email address for Teams membership.

4. Teams site Owners must not accept any email that doesn't look like a person e.g. shared accounts where the password is known to more than one person.

5. Ensure that Members and Guests understand your expectations for how they will use your Teams site and that they are aware:

    a. That information held within the Teams site is subject to data protection legislation and could be asked for in order to respond to an information access request such as a Subject Access Request and so the same level of care regarding the content should be taken as with other University records and correspondence

    b. How to contact site Owners for guidance if needed

6. In addition, for Members, ensure that they are aware:

    a. whether there are Guest members of the site

    b. what type of information it is appropriate to share on the site

After granting access

1. As an additional precaution, arrange to regularly (at least annually and more often if the nature of the content requires this) review:

    a. the membership of your site

    b. the assessment of the information in your site against the UK consolidated strategic export control list to ensure that no “coded” information has been added. If “coded” information is identified in these yearly reviews, you must inform the Regulatory Compliance Team regulatory.compliance@manchester.ac.uk. (See section E below.)

    It will be good practice to keep a record that these checks have been performed somewhere that all site Owners can access it.

2. Ensure that access is removed promptly when no longer required.

E. Export controls

1. As site Owner you are responsible for all exports that take place in your Teams site.

2. Enabling access to information for someone located outside the UK border is considered an export.

3. Similarly, enabling access to information for someone who is currently located within the UK but whose home institution/organisation is located in a key country may be considered providing technical assistance under export controls.

4. Some Guests may not be permitted access to information which falls under export control legislation or other funder, legal, regulatory or statutory requirement in respect of processing data and information.

5. Member and Guest access to your Teams site may only be provided after export clearance has been received from the Regulatory Compliance Team regulatory.compliance@manchester.ac.uk. **Note:** make sure you keep the export outcome letters for auditing purposes.

6. It will be your responsibility to:

    a. put in place an export licence if Guests proposed for access to a Teams site are outside the UK and are associated to an organisation located in Key countries).

    b. submit a request for export clearance via the online form to the Regulatory Compliance Teams prior to giving access to a Guest, and not to grant them access until clearance has been issued.

    c. request checks on the Guest's home institution where needed (e.g. https://www.staffnet.manchester.ac.uk/export-controls-info/collaborators-funders/sharing- collaborators/)

Further information can be obtained from the Regulatory Compliance Team by emailing regulatory.compliance@manchester.ac.uk.

This document is stored and maintained here:
https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=53167