Team Owner responsibilities

Prerequisites:
- [Highly restricted information](#) must not be shared or stored within the Teams platform or Team sites.
- Information to be shared with individuals from organisations which are subject to export control legislation must not be included without clearance. (Where the Team sites are to be used for international collaboration, the Team Owner must request [checks](#) on the entity they plan to grant access if their home institution is located in a [key country](#)).

The Team Owner for a Team site is responsible for the following:

Managing access to the Team site:
- Ensuring that the Team site has a minimum of two Owners who must be members of staff at the University. Only two Team Owners are permitted to be able to invite guests to a Team site.
- The Team site is set as Private by default and must not be changed to Public. Private teams can only be joined if the Team Owner adds someone to them. Public teams are visible to everyone from the Teams gallery and can be joined without getting approval from the Team Owner.
- Ensuring that member and guest access to the Team site is only provided where necessary and is removed promptly when no longer required.
- Ensuring that the email addresses of members added to the Team are accurate, otherwise there is a risk that access to the posts and files within the Team site is given to unauthorised people. The search list which is used to select new members may not have sufficient information to accurately identify people, so, if in doubt, email the individual concerned before granting them access. Additional due diligence is required in relation to guest members of the Team (see below).
- Reviewing Team Owners, Guest Inviters, members and guests of the Team at least annually to ensure that they are still valid.
- Responding to actions resulting from any audits or alerts in relation to the Team site.
- If a person leaves the University who is an Owner of an existing Team, the second owner of the site is responsible for delegating another suitable Owner and ensuring that access to the leaving owner is removed. This should be done in an informed and agreed manner before the delegated user is assigned the role of Owner.
- Whilst the Team Owner can add a new Owner to the Team, if the new Owner will need to be able to invite guests to the Team a request must be submitted as a "Microsoft Office 365 request" via the [IT Services Support Portal](#) for access to the Guest Inviter role.

Inviting guests to the Team site:
- 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 which have access to University data. University staff must only use their University email address for Team membership. Team 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.
- Where necessary, when creating the guest account, the Team Owner should edit the guest's display name so that the individual can be identified.
- Where a Team Owner wishes to provide access to a guest (i.e someone who doesn't have a University of Manchester IT account) it is the responsibility of the Team Owner to confirm the identity of the guest i.e. that they really are who they say they are and to request appropriate due diligence checks. Failure to do so could mean that unidentified individuals gain access to the posts and files within the Team.

- When a guest is first added to any Team an account is created for them. This means that their name will then appear in the search list and could be selected by any Team Owner. However, inclusion in the list doesn't mean that it is appropriate for the guest to have access to any other existing or new Team sites and appropriate due diligence must be taken by the Team Owner to confirm the identity of guest selected from the search list.
- It may be necessary for there to be a contract in place before adding a guest eg where controlled information may be involved. For example, personal information (eg 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. Similarly, 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. It is the guest inviter's responsibility to request checks on the guest's home institution where needed (eg https://www.staffnet.manchester.ac.uk/export-controls-info/collaborators-funders/sharing-collaborators/) and it is their responsibility to not grant them access until clearance has been issued. It is the guest inviter's responsibility to put in place an export licence if guests within a team are outside the UK. Further information can be obtained from the Export Control team by emailing ecc@manchester.ac.uk.
- The Team Owner is responsible for ensuring that guests are aware of the key policies and procedures which apply to the use of Teams (see below).
- It is important to be mindful, that once they join the Team, guests may be able to see all chats, posts and files shared within the Team channels to which they have access, including historic chats and information.
- The Team Owner must ensure that Team members are aware of any data which cannot be shared with guests.

Managing information in the Team site:
Team 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 but specifically in relation to Team sites this includes:
- Sharing Information within a Team appropriately to minimise information risk. This would include sharing SharePoint links to 'Team members', 'Specific people' and /or allowing Editing or downloads.
- Ensuring that all data stored or processed within a Team are compliant with data protection legislation and any relevant data sharing agreements and contracts, and must adhere to the mandatory requirements set out in University Standard Operating Procedures as applicable to the Team site, in particular:
    - Information Security Classification, Ownership and Secure Information Handling
    - Document and Information Management
    - Acceptable Use of IT Facilities and Services – SOP for Staff (including guests)
    - Acceptable Use of IT Facilities and Services – SOP for Students
    - Privacy guidance when recording meetings
  The content of Teams files, chats, recorded meetings etc may need to be obtained in order to respond to information requests, so the same level of care regarding the content should be taken as with other University records and correspondence.
- Some contracts may have constraints on where information can be stored and how it must be protected. The Team Owner must ensure that information stored in Teams is compliant with these requirements. Information regarding the location of information stored in Microsoft 365 can be found here https://www.staffnet.manchester.ac.uk/modernising-it/technology/office365/teams/faqs/

October 2021

- Ensuring that any important records in the Team site are appropriately protected, for example from accidental amendment or deletion. Consider creating [alerts in order](#) to be notified of any changes.
- Where necessary, providing guidance to members of the Team to support them to use the site appropriately.

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