APM Terms of Use for Microsoft Teams & SharePoint

PLEASE CONFIRM THAT YOU HAVE READ THESE TERMS OF USE CAREFULLY BEFORE USING MS TEAMS and SharePoint.

Your use of this system means that you agree to these terms of use. If you do not agree to these terms of use, please contact the administrator for each area.

User Responsibilities

1. Personal information, including contact email addresses, stored in this system **must only be used for matters directly related to APM volunteering activities**. The information must not be used for non-APM business such as advertising of events, job vacancies, or the services of third-party organisations, regardless of their commercial status. If you are in any doubt about the eligibility of a proposed communication, then you should seek advice from the APM administrator before sending .

2. The system may contain personal data governed by GDPR. This includes contact details which are provided solely for business use in connection with the work of the team and are not for further or wider use without explicit consent. A detailed guidance note for volunteers on data protection issues is available in the Volunteers team area and on request from dataprotection@apm.org.uk.

3. It should be assumed that the documents and files stored in this system are confidential, and must not be distributed, unless explicit instructions or authorisation to the contrary are provided.

4. Good housekeeping of folders and files are essential and users must follow the structure set out by the APM administrator

5. Individual team members are responsible for ensuring that their contact details are kept up to date at all times to ensure they continue to receive communications.

6. Individual team members must adhere to the IT Security advice set out below and the 'Data Protection Guidance for Volunteers' available via a MS Teams Group or SharePoint site
7.
8. Permission to record meetings must be obtained prior to any meeting.

APM Administrator /Main Owner Responsibilities

9. The APM administrator / Main Owner for each area will be responsible for:
   - issuing invitations to individuals to become members of the Microsoft Team / SharePoint site.
   - removing unregistered users who have not created an account within 2 months of their invitation to register

- ensuring that all users have the appropriate level of access to folder contents. This means that they will only have access to the information necessary for them to fulfil their role. Any more confidential information will be stored in a separate folder with access restricted to those necessary.
- removing the accounts of users who have been inactive for 12 months or more
- addressing any queries raised by members of the Microsoft Teams/SharePoint site in relation to accessing the files/folder. The APM administrator / Main Owner will be tagged under the 'Manage Teams" section of the Microsoft Teams
- arranging for the archiving and closure of the Microsoft Teams files/folder.
- liaising with IT support or APM's line management to resolve any issues with the administration of the area
- Determining retention period of documents, meeting recordings and folders and ensuring they're added to the APM Retention Schedule (please let the DPO know)
- Deleting or anonymising documents/recordings at the end of the retention period
- Maintaining good data governance

Intellectual Property

10. The names, images and logos identifying APM or third parties in their products and services are subject to copyright, design rights and trademarks of APM and/or third parties. Nothing contained in these terms should be construed as conferring by implication, estoppel or otherwise any licence or right to use any trademark, patent, design right or copyright of APM or any third party. In short, you should also assume that APM owns the copyright in any material which it has placed on the system. Always check if you intend to reuse any material.

General Terms

11. APM may change these terms at any time by notification via the system and your continued use of the system after such changes have been notified means you agree to be bound by these terms as amended.

IT Security Controls

12. APM does not warrant that functions contained in the system are error free or free of viruses or bugs. Users must take every effort to comply with the following:
    a) Ensure that all devices used to access the system have 'front end security'. For example, a password or fingerprint must first be used to access the device.
    b) Devices should lock themselves after a period of five minutes inactivity
    c) Passwords set to create a Microsoft account should be 'complex'. i.e. at least eight characters and include a mixture of upper and lower case letters and symbols. Passwords should be changed at least every 90 days and never be identical or similar to any other passwords you use.
    d) External users and those accessing on non-APM equipment should log in and out of the system at each use.
    e) Devices should have recognised security software installed. For example, Sophos, McAfee.
    f) If in doubt, please follow the UK's National Cyber Security's Centre's advice on how to stay secure online here,

For added security and in line with our Cyber Security Essentials requirements, we will be rolling out Multi Factor Authentication. Please let us know if you have any questions or issues. More information will follow.

Version 4 – April 2024