Terms of Use and Data Protection Guidance for Volunteers

Content

1. Scope and Introduction
2. Using Zoom and its AI Features
3. Using Microsoft Teams & SharePoint
4. WhatsApp and Instant Messaging Guidance
5. IT Security Controls
6. Frequently Asked Questions and APM Support for Data Requests
7. Intellectual Property
8. General Terms
9. Appendix 1: Data Protection Principles
10. Appendix 2: Data Protection Top Tips

1. Scope and Introduction

This guide is designed to support you as an APM volunteer by showing how staff can assist you in your role. It provides clear, practical advice on managing data responsibly, answers to frequently asked questions, and guidance on using digital tools securely and compliantly. Inside, you'll find best practices for Zoom AI features, Microsoft Teams, and SharePoint, as well as tips for using WhatsApp and other instant messaging platforms in line with data protection standards.

Introduction

Personal data is about you. It is anything that relates to you as an identifiable individual. It's not just your contact details but can include your finances, your health, your views, opinions and preferences. Data protection is about protecting you from the misuse and mistakes others might make with your information. But it is also about the personal data of others that you handle.

The personal data managed by volunteers on APM's behalf needs to be given robust protection and be processed fairly in accordance with UK GDPR (The UK General Data Protection Regulation) principles. This necessitates some sensible and proportionate controls on access and use which are set out in this document.

Our overriding aim is to manage personal data in accordance with the UK GDPR. Remember, APM must protect YOUR personal data to the high standards you would expect. A failure to do so creates regulatory risks but more importantly can irreparably damage the reputation of APM with its members and stakeholders. As volunteers, you may at times be handling personal data on behalf of APM. It is therefore your responsibility, as well as APM's, to ensure that all personal data is managed and protected in line with GDPR requirements.

Overarching Principles

- APM staff and volunteers must exercise caution when using personal data.
- Always be sure that you have the right to use the data for the intended purpose.
- Always ensure you understand the requirements and check if unsure.
- Always make sure that data is stored and transmitted securely.
- Ask yourself if you would be happy with your data being used in this way? Are you comfortable that all others would feel the same?
- For data quality and data security, APM should manage central lists with the main database

(CRM) being the ‘single source of truth’.
- Formal communications such as invites to events should be made by APM.

Reference Material and Background

- The key data protection principles are largely common sense. See Appendix 1 – make sure you understand and apply them. Always check if you are unsure.
- Some generic ‘top tips’ to help you think about how to protect personal data are included in Appendix 2.
- The APM website’s privacy statement sets out how we manage personal data. Please read it.

2. Using Zoom and its AI Features

This section applies only to Interest Network volunteers, as Zoom is the approved main platform for Interest Network meetings and activities. Regional Networks continue to use Microsoft Teams, and separate guidance is provided for those groups below.

It relates to all Zoom tools and features made available by APM, including Zoom’s built-in AI Companion.

To discourage the use of external AI tools, which often store data outside the UK/EU and are not under APM’s control, APM has enabled certain Zoom AI Companion features within our secure environment. Data generated through these features is stored securely in Zoom's EU data centre (Germany) alongside other APM Zoom content. These features may support meeting summaries or collaboration when activated, but they are only used under APM’s centrally managed settings and retention rules. AI functionality does not activate automatically; meeting hosts must choose to enable it for a session.

APM strictly prohibits the use of third-party AI note-takers or transcription tools in any online meetings.

General Best Practices

- Data Protection: Always adhere to data protection policies and ensure that any personal or sensitive information is handled securely.
- Transparency: Using AI to create Zoom meeting summaries is an option, However, be transparent with your team about the use of AI features and allow for alternative options if a member wants to opt out of the use of recordings / AI (i.e. by not recording/transcribing a meeting)
- Feedback: Please provide us feedback on the AI features to help improve their accuracy and usefulness.

Meeting Notes/Summary for Chats, Recordings, and Meetings

- Permission to record meetings must be obtained prior to any meeting and attendees must be informed if the transcript will be used to generate an AI-generated summary.
- Always ensure that the content discussed in meetings is kept confidential. Do not share meeting summaries or notes with unauthorised individuals.
- Zoom recordings and transcripts are not automatically available to meeting attendees. Access is restricted to authorised hosts and administrators and will only be shared where appropriate and in line with APM guidance.
- Meeting notes generated by the Zoom AI tool should be exported and stored in SharePoint (which remains the main repository) after each meeting. AI minutes are only stored in Zoom for 30 days (see below).

- Automated retention rules apply as below to any date recorded in Zoom:
    - Meeting minutes (AI Generated) stored in Zoom: 30 days
    - 1 to 1 chats and group chat content is kept for 1 year
    - Meeting recordings and associated transcriptions: 6 months
- Review the AI-generated summaries for accuracy. Make any necessary corrections before sharing them with the team.
- External and unapproved AI Summary bots are prohibited in Zoom. Any external tools used to generate an AI-generated summary of a meeting must be approved by APM before use.
- Refrain from discussing private or sensitive personal information during meetings.

Virtual Whiteboards

- Use the Whiteboard feature to brainstorm and collaborate. Ensure that all content added is appropriate and relevant to the discussion.
- Utilise AI to help organise ideas and content on the Whiteboard. This will make it easier for everyone to follow along and contribute.

Do not share sensitive or confidential information on the Whiteboard. Treat it as a public space where all participants can see the content.

3. Using Microsoft Teams & SharePoint

This section applies only to Regional Network volunteers, as Microsoft Teams and SharePoint are the approved platforms for Regional Network communications, meetings, and document storage. Interest Networks use Zoom, and separate guidance is provided for those groups.

APM uses Microsoft Teams and SharePoint because they offer a secure, centrally managed environment for collaboration, with strong controls over access, storage, meeting permissions, and data protection. To maintain compliance with APM's data protection and security standards, Regional Network volunteers must not use any unapproved or personal AI tools, including external AI meeting summary bots, transcription assistants, or third-party apps, in connection with APM activities. Only APM-approved Microsoft 365 features may be used.

User Responsibilities

- 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.
- 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.
- 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.
- Good housekeeping of folders and files are essential, and users are responsible for deleting emails and files when no longer necessary. Users must follow 'the issued Housekeeping Guidance'.
- 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.
- Individual team members must adhere to the IT Security advice set out below and follow The Volunteers Handbook.
- Permission to record meetings must be obtained prior to any meeting and attendees must be

informed if the transcript will be used to generate an AI-generated summary.
- Automated retention rules apply and MS Teams Meeting recordings and associated transcriptions are kept for 6 months
- 1 to 1 chats and group chats are kept for 18 months in MS Teams after which they'll be automatically deleted.

External and unapproved AI Summary bots are prohibited in MS Teams to ensure compliance with our data protection and security standards. Any external tools used to generate an AI-generated summary of a meeting must be approved by APM before use.

APM Responsibilities

- 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 identified as an inactive volunteer for 6 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.

4. WhatsApp and Instant Messaging Apps Use Guidance

At APM, we encourage volunteers to use APM-provided messaging tools whenever possible because they help keep information secure, protect personal data, and maintain clear boundaries between volunteering and private life. While apps like WhatsApp may seem convenient, messages on personal platforms can be stored outside APM's control and blur work-life balance. If no APM channel is available and urgent contact is required, these apps can be used in exceptional circumstances - but please keep this to a minimum. Using apps like WhatsApp is a personal choice and never a mandatory step as an APM Volunteer.

The principles below apply to all social media and messaging apps, not just WhatsApp.

Our aim is to help you understand how to use these tools only if absolutely necessary, to ensure compliance, safeguard everyone's privacy, and protect APM's data. If you have any concerns or questions about the use of WhatsApp, please contact volunteers@apm.org.uk.

Guidance For All Volunteers

The following guidelines apply when using WhatsApp or any social media / instant messaging:

Do	Don't
Use WhatsApp only when alternative tools provided by APM (such as Teams, Zoom or Outlook) are insufficient for your needs	Don't share personal data, sensitive, or confidential information (e.g. volunteer details, matters, financial data)
Keep messages brief and factual	Don't use WhatsApp as your main volunteering communication tool
Make sure your participation in WhatsApp groups is voluntary. There should be no pressure to join or use your personal device	Don't send or feel obliged to respond to messages outside your intended volunteering hours - this helps keep boundaries and avoid stress.
Let your Network Lead or the APM DPO know if you have concerns about WhatsApp use or feel pressured to participate. This will be kept confidential	Don't add volunteers to WhatsApp groups without their consent
Use secure, approved channels (Teams, Outlook, RingCentral) for all routine, sensitive, or confidential work communications	
Remember to delete volunteer-related WhatsApp messages and files from your device when they're no longer needed	
Check and update your WhatsApp privacy settings to enhance your protection. There are simple steps you can take to keep your data private and secure.	
Respect others' availability and capacity - do not expect immediate responses and be understanding if someone cannot reply straight away.	

<u>Guidance For Network Leads and Deputies</u>

The following guidelines apply when using WhatsApp or any social media / instant messaging:

Do	Don't
Use WhatsApp only when alternative tools provided by APM (such as Teams, Zoom or Outlook) are insufficient for your needs	Don't *require* volunteers to use WhatsApp. It must be voluntary, and alternatives should be offered
Make it clear to everyone that WhatsApp use is voluntary and not a requirement	Don't use WhatsApp for ongoing volunteering messaging. Use the tools provided by APM
Obtain consent before adding anyone to a WhatsApp group – never ask for consent in a group setting	Don't store or rely on WhatsApp messages for business records—use approved systems for record-keeping
Remind the group you manage not to share sensitive or confidential information via WhatsApp	Don't ignore concerns raised by volunteers about WhatsApp use

Regularly review whether WhatsApp is still fit for purpose	
Offer alternatives and support for those who prefer not to use WhatsApp	
Encourage your group to respect each other's availability and capacity to respond and remind everyone that prompt replies are not always possible or can be expected.	
Remind your group to delete volunteer-related WhatsApp messages and files when they're no longer needed	
Handle any sensitive data shared with great care*	

*If you inadvertently receive sensitive personal data (such as medical information) via your personal phone, you should:

- Promptly transfer the information securely to an approved APM system (such as Outlook or SharePoint) if it is needed; otherwise, promptly delete it.
- Delete the message and any attachments from your device as soon as the information has been securely stored.
- Inform the individual (if appropriate) that, for their privacy and security, such information should be sent via approved channels in the future.
- Contact APM IT or DPO for advice if you are unsure how to handle or store the information securely.

What are the risks?

- Personal phones prevent us from fulfilling data access or erasure requests as we have no control
- Files shared may end up on personal devices or cloud backups outside APM's control
- Sharing phone numbers or profile photos with other volunteers who you may not know may feel intrusive, and some volunteers may feel pressured to share details they'd rather keep private
- WhatsApp is usually for friends and family. Using it in a professional capacity can blur boundaries, making it harder to switch off and increasing stress - especially if messages are sent outside usual hours

Need help or have concerns or questions?

Please feel free to contact the APM Volunteers Team or the APM DPO.

5. IT Security Controls

APM does not warrant that functions contained in the system are error free or free of viruses or bugs. Users must make every effort to comply with the following:

- Multi-Factor Authentication (MFA) is now the most important security measure. Unlike regular password resets - which can actually increase risk if users choose weaker passwords - MFA adds an extra layer of protection by requiring something you know (your password) and

something you have (like a code sent to your device). This makes it much harder for attackers to gain access, even if a password is compromised. If you experience any issues with MFA or need help accessing your account, please contact the IT team for support.

- Ensure that all devices used to access APM systems have 'front-end security'. For example, a password, PIN, or fingerprint must first be used to unlock the device.
- Devices should lock themselves after a period of five minutes of inactivity.
- Passwords for your Microsoft account should still be complex (at least eight characters, including a mix of upper and lower case letters, numbers, and symbols).
- External users and those accessing on non-APM equipment should log in and out of the system at each use.
- To ensure secure and reliable access to APM systems, volunteers must use devices with recognised security software installed, such as Sophos or McAfee. If in doubt, please follow the UK's National Cyber Security's Centre's advice on how to stay secure online.
- Third-party AI note-taking tools (such as Otter.ai, Fireflies, etc.) are not permitted for use with APM systems, including Microsoft Teams and SharePoint. This restriction is in place to protect sensitive information and ensure compliance with our data protection and IT security standards. Only APM-approved tools may be used for meeting notes and transcriptions. We are actively exploring alternative solutions to support volunteers' needs while maintaining robust security.

Why this matters:

These controls are essential to protect both volunteers and APM systems. They help prevent unauthorised access, reduce the risk of data breaches, and ensure compliance with cyber security standards. Features like device passwords, automatic locking, complex account credentials, and recognised security software create a secure environment for accessing APM systems. Without these safeguards, critical functions such as MFA may not work properly, leaving systems vulnerable to malware, phishing, and other cyber threats. By following these requirements, volunteers help maintain system integrity and keep sensitive information safe.

6. Frequently Asked Questions and APM Support for Data Requests

The following sets out the answers to common queries and how APM can support volunteers' data requests and queries.

Common questions and queries	Answers and how we can support you
Can I use and store my own contacts?	There is no bar on individuals sensibly managing their own contacts. There is no problem if you hold contacts in your email software (e.g. Outlook) of people who you know are happy to be contacted. Where someone has agreed to be contacted by you then you can go back to them on related matters. Of course, you still need to be careful about what you use their data for and to whom it can be passed. Seek guidance if unclear and refer to the DPA principles in Appendix 1. Regional Networks and Interest Networks must not maintain local lists or databases of personal data, for example, contact lists of corporate partners or event attendees (see below). Regional Network and Interest Network Leads and Deputies can maintain email distribution lists of team members in order to arrange meetings etc. Regional Network and Interest Network Leads and Deputies are responsible for managing meeting invitations. This task may be delegated to a coordinator, but accountability remains with the Lead and Deputy. Only volunteers included on the APM-provided volunteer list may be invited to meetings. Meeting invitations and meeting links must not be forwarded or shared with individuals who are not on the approved attendee list. Updated lists of active volunteers are provided by APM.
Can the Regional Network / Interest Network maintain our own lists of personal data? For example, local corporate contact details.	Apart from as detailed above - no. Access and use to member and corporate personal data must be managed in accordance with UK GDPR principles. Data quality and security is compromised if it is held locally and there can be no assurance over its use. There must be one 'source of the truth' which is updated centrally and this is APM's CRM database.
I need the most up-to-date contacts in order to send out an invitation to an event?	All invites to events must be centrally managed by APM. This ensures that the invite goes to the most up to date contacts. You can forward the invitation to any personal contacts.

I think I have more up-to-date details than APM. Can you update the central database with them?	Please pass on the details and we will check. If there is a discrepancy we will check with the individual and update the database. We may ask you to encourage the individual to contact us directly or to register or update their account on the website. If they are not on the database, we can't assume that because they have given you their details that APM can add them to the database. For example, we need their specific preferences on the database to market to them.
I want to discuss an opportunity with local corporate partners and affiliates. Please send me their details. Please can you advise the best contact at an organisation? I used to deal with XXX at XXX but they don't respond. Can you give me another contact?	We know that many corporate contacts are very protective of their data and do not want their details passed on widely. Several have refused to have them passed on and we must respect their right to say no. If you are happy to pass your details to them, we will forward on and encourage them to make contact if they wish.
Is XXX a corporate partner/affiliate /HEI?	There is a list on APM website which is always kept up to date.
Is XXX an individual member of APM? Is XXX an RPP? Is XXX a ChPP?	RPPs and ChPPs have public registers which they can opt into and which can be searched on the APM website. Honorary Fellows are also listed on the website. There is no public register for individual members (students, associates, MAPMs and FAPMs) and we can't release individuals' status without their consent; which might be appropriate to source.
How many people did our email go to?	APM can provide stats on the number of emails sent and the CTOR (Click To Open Rate).
Can we have a copy of the delegate list?	It is common practice to share delegate lists with those attending for personal networking – these comprise name and company. Individuals have the right to opt out of this. Contact details are not shared more widely with Regional Networks, Interest Networks or sponsors and speakers. Remember that the data should not be held locally and the data is unlikely to be available for secondary use. Please discuss with us what you want to do and if there is another way to help.

Can APM ask its members if they give consent to be contacted by their Regional Network or Interest Network representative? If they consent, can we make contact direct?	Communications about events and formal opportunities can be managed centrally and we can email them directly on your behalf. Managing consent is complex and there would need to be a process for storing consent and a process for its review and removal. Regional Network and Interest Network officers can be contacted via the website and we can encourage people to get in touch with you. We are happy to pass your details to them.
The CRM doesn't easily store the various local / regional offices of corporate partners. How can we manage this?	This is a known issue which is being examined. APM staff will be able to manage a central 'work around' and support you with your needs. Please ask for assistance.
Is MS Teams and SharePoint secure?	A connection between your device and MS Teams is considered to have suitable levels of IT security. Please do not download and store any personal data locally. You should have a password, username, or PIN controlled access to your device. For added security, we have now implemented Multi Factor Authentication. .
Are there any restrictions on using the contact details in MS Teams?	Yes, Individuals give their contact details for APM volunteer business and there should be no wider use. APM administrators (Main Owners) for each individual MS Teams area should review and maintain the content of each project. This should include deleting users who are no longer active and data that's no longer necessary.

7. Intellectual Property

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.

8. General Terms

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.

9. Appendix 1: Data Protection Principles

- Processed lawfully, fairly and in a transparent manner in relation to individuals (i.e. can we do this and is it reasonable? Does the individual know?).
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (i.e. only used for the purpose collected).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (i.e. only keep what you need).
- Accurate and, where necessary, kept up to date (i.e. keep it accurate).
- Not kept for longer than is necessary (i.e. check but delete what we don't need).
- Processed in a manner that ensures appropriate security (i.e. look after it).

10. Appendix 2: Data Protection Top Tips

DO's	DON'Ts
DO ensure you have an agreed process and approval before sharing personal data or using it for a new purpose. Always consider privacy issues when creating new procedures and check with APM if unsure.	DO NOT forget information is a key asset we cannot afford to lose. The trust of our customers and significant fines are at stake.
DO make sure you double check before sending emails that you have entered the correct recipient.	DON'T include multiple email contact details in the 'to' or 'cc' fields – protect email addresses wherever necessary by using the 'bcc' field.
DO ensure personal data is secured in transit by encryption using secure passwords and secure FTP sites. Check with APM if you are unclear.	
DO create lengthy passwords (9 characters or more) containing both letters, numbers and symbols. Choose something which makes sense to you but is not easy to guess.	
Save files to network drives and not to local hard disks. Do not use memory sticks or laptops unless they are encrypted (APM standard) and this process has been approved.	
DO read the APM Privacy Statement and the above Terms of Use before using MS Teams, SharePoint, WhatsApp or any other collaborative or messaging tool.	