Guidelines for volunteers when handling personal information

With the introduction of the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018, RPS has been reviewing and updating its policies and procedures around the handling of personal information. This guidance is centred around the key principles of the above legislation and is intended to give volunteers confidence about the way they handle personal data and to give RPS assurance that personal data is being managed appropriately, and therefore not exposing the organisation to undue regulatory or reputational risk.

The RPS has assessed the way data is stored and used with the assistance of an independent data protection consultancy. These guidelines have been written based upon an assessment of risk and proportionate steps that should be taken to protect personal information. All volunteers should be familiar with these guidelines, and may also find it helpful to read our general Privacy Policy at **http://rps.org/about/terms-and-conditions/privacy.** If in doubt at any time, please contact the Volunteering Team or email **dataprotection@rps.org**

Purpose

- Personal information must only be used for specific defined purposes that individuals are made aware of. Our core Privacy Policy (http://rps.org/about/terms-and-conditions/privacy) contains most of these purposes but there may be times when additional notification is required i.e. where there is a new or different use of personal information.

Accuracy

- Personal information provided to volunteers at a point in time can become out of date quickly. To ensure accuracy of personal information being used, volunteers should request fresh data from RPS headquarters when required from the Volunteer and Member Support Coordinators, IT Manager or other appropriate staff members.
- Do not maintain separate duplicate lists of personal information that may not align with the central database.

Access

- Access to personal information should be limited to only those people who require access as part of the role they are fulfilling e.g. a Membership Coordinator.
- To ensure we have good records in the event of a loss of personal information, or a breach of information security, RPS headquarters will keep a record of what data has been passed to volunteers to be able to carry out necessary follow-up actions.

Security

- Ensure any computers, tablets and smartphones used to hold or access personal data are running the most up to date operating system and security updates.

- Email is the cause of many information security breaches so, where possible, always view or share documents from source rather than sending copies via email e.g. access via Office365/Sharepoint or a similarly robust/compliant platform.
- Personal information should always be limited to the minimum data that is necessary for the purpose. For example, if you only require a name and a phone number for an event, that is all that should be collected.
- Files with large amounts of personal data should be stored/transferred with password protection, and passwords communicated separately.

Retention

- Personal information must only be kept as long as it is required. If there is no longer a need for it, delete all copies as soon as possible e.g. after an event has taken place. Consider copies held in multiple locations.
- Volunteers should ensure all files are passed on and/or deleted (as appropriate) when they leave a role (this is covered in the new formal process for volunteer starters and leavers).

Loss of personal information or complaints

- If you receive a complaint in relation to the handling of someone's personal information, please contact dataprotection@rps.org as soon as possible to discuss the issue and any follow-up steps required.
- If any personal information in your possession is lost or stolen (whether paper copies or held on an electronic device), please contact dataprotection@rps.org as soon as possible.

Communications

- It is an individual's choice as to what types of communications they want to receive especially where this constitutes direct marketing e.g. advertising events or promoting an organisation's aims and beliefs.
- Use of RPS contact information must relate to RPS business, and such information must not be used for other purposes unconnected with RPS.
- Wherever possible and practicable, the central RPS broadcast system should be used to send emails relating to RPS activities.
- Where emailing a group of people independently, always consider the security of the email addresses and whether it is appropriate for them to be shared within the group. Use the "bcc" field whenever possible e.g. if the recipients' or their email addresses are not already known to each other.
- If using a third-party emailing service, you should use a European based provider such as:
  - FreshMail
  - E-goi
  - Sender.net
  - SendinBlue
  - Moosend
  - Minutemailer
  - Mail Chimp
  - GetResponse
  - UserEngage.io
  - MailerLite
  - Sendy
  - Adestra
  - Smartmessages
  - Mautic

Document control

Document title	Guidelines for volunteers when handling personal information
Filename	RPS DP volunteer guidance.docx
Version number	V2
Approved by	Dan Jones, CEO
Approval date	23 March 2023
Review date	24 months after approval date