SWF Information & Data Protection Policy

The Data Protection Act 1998 requires every data controller who is processing personal data to notify unless they are exempt. Failure to notify is a criminal offence. SWF has set up a direct debit to renew our notification each year for the following purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Administration of membership records
- Advertising, marketing and public relations for others
- Consultancy and advisory services
- Education
- Fundraising
- Information and databank administration
- Journalism and media
- Legal services
- Processing for not for profit organizations
- Realizing the objectives of a charitable organization or voluntary body
- Research
- Trading/sharing in personal information

If SWF needs to collect data for any purpose not stated above we should notify the Information Commissioner before collecting that data.

Eight Data Protection Principles

Whenever collecting information about people SWF agrees to apply the Eight Data Protection Principles:

1. Personal data should be processed fairly and lawfully
2. Personal data should be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required
4. Accurate and kept up-to-date
5. Data should not be kept for longer than is necessary for purpose
6. Data processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organizational measures should be taken unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EEA unless that country or territory ensures an adequate level of data protection.

Notes for SWF*:*

- Data controller must provide their identity, people should be told exactly what the information is being collected for and any other information necessary. We must get their consent.
- We should think in advance about what we wish to do with personal data – i.e. – if we get names and addresses for a specific event we should only use that info for that event – we should from now on add other purposes to forms – e.g. I wish to be kept up-to-date with SWF's activities.
- Individuals have a right to see what data is being kept on them, and for what purpose, requests should be in writing to the data controller giving 7 days' notice.
- Same principals need to apply when data is taken out of the office.
- If we buy in a mailing list we cannot use it for any other purpose than the original Data Controller has specified – we must check original use.

Working from home

- SWF keeps note of which staff take work home with them
- If working on something at home and at work try to keep both sets of information pretty much up to date
- Home computers should have records removed once project/work records no longer needed at home
- Staff agree to try to keep work taken home relatively secure, to return all work related material upon the completion /termination of their contract; and organization should be informed if information have got into wrong hands

Special funding tracking requirements and data protection

- Try not to keep more than project/tracking requires
- The more information kept the more secure it should be kept
- If publishing volunteers' details, tell them
- Take extra care if records include sensitive data
- Just keep personal data as long as necessary under funding rules
- Don't keep surplus information.

Security Statement

SWF has taken measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage. In pursuit of that, we have migrated our data from hybrid on prem/private cloud infrastructure to Microsoft 365. This has allowed implementation of conditional access via MFA for all staff, and improved device management. We will continue to leverage features and improvements available in our M365 environment, with the current license type deployed. When suitable backup solution is implemented, it would be envisaged that it would be a cloud-to-cloud solution. Until then manual data copies will be taken to encrypted external hard drives and held in safe location off site. Other actions include detecting and investigating breaches of security should they occur