Data Protection & IT Security Policy for SHAPA

Issue 1 : March 2018

About this policy

This Data Protection and IT Security policy applies to all operations of Shapa.

The policy is designed to ensure that Shapa complies with its obligations under the Data Protection Act (to be replaced with the General Data Protection Regulation (GDPR) in 2018) and conforms to the following eight data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The General Secretary is the owner of this policy and responsible for its regular review (at least yearly) and update as necessary.

The personal data we hold

Data description	Personal data included	Stored using	Retention policy	Responsible officer
Information about our members	Contact information, appointments, training records, and awards.	Office 365	Retained whilst a current member. A subset of data is retained	General Secretary

	(Includes sensitive data, as defined)		when a membership ceases in order to support the vetting policy should the person reapply for membership	
			10 years	General Secretary
Information about our employees where applicable	Applications of jobs where candidate is unsuccessful	email	6 months after notifying candidate	Chair
	Contact details, start dates, annual leave, TOIL, contract, references, copy of other relevant documentation (e.g. disciplinary letters) *(Includes sensitive data, as defined)*	Proactive-HR system (provided by 3rd Party)	5 years following the employee leaving employment	Chair
	Contact details, salary and pension contribution information		Indefinitely	Chair
	Copies of right to work checks, certificates and other physical documentation provided by employees	Employment files stored in office 365	5 years following the employee leaving employment	Chair
	Payroll information, including salary and other allowances, P60, P45, P11D and P6 notices.	SAGE, stored on on-site server	7 years	Chair

For completeness, we also hold the following information which is not categorised as Personal Data but has the following retention policies applied:

Data description	Retention policy	Responsible officer
Finance – purchase ledgers, record of payments made, invoices, bank paying in counterfoils, bank statements, remittance advices, correspondence regarding donations, bank reconciliation.	7 years	General Secretary
requests removal	10 years	General Secretary
requests removal	Indefinitely	General Secretary
Annual accounts and annual reports	Indefinitely	General Secretary
Insurance policies	Indefinitely	General Secretary
Employer's Liability insurance certificate	40 years	General Secretary
Health and safety records	3 years	General Secretary
Contract with customers, suppliers or agents, licensing agreements, rental/ hire purchase agreements, indemnities and guarantees and other agreements or contracts	6 years are expiry or termination	General Secretary

Our Security Policies

The following security policies will apply to the storing of personal data as outlined in this policy. These security policies are mandatory.

Overarching policies

- **Need to know** – We only give people access to the data that they need to carry out their role. If people change roles, we review access accordingly.
- **Commercially available software** – where possible we use third party software to store personal data (either installed on our corporate IT network or provided as software-as-a-service), where the software is regularly testing and patched for security vulnerabilities.
- **Employment** – We ensure our employees are made aware of their data protection obligations through clauses in their contracts and details contained in the staff handbook.

- **Transporting data** – We only transport data using physical media if absolutely necessary and then using encrypted media only.
- **We keep people informed** – we tell people why we are collecting their data and how we use it, at the point in time we collect it.

Physical storage

- **Limiting storage** – We limit the amount of personal data we physical store to the absolute minimum. Only those with a need to know will have access to the data.

Corporate network

- **Boundary security** – Our corporate IT network at SHAPA shall have a boundary firewall which restricts inbound access to those ports and protocols specifically approved, which is maintained and supported.
- **Internet filtering** – All internet traffic (including public Wi-Fi) shall be filtered to ensure that inappropriate websites cannot be accessed.
- **IT Security patching** – The latest available IT Security patches are installed regularly and automatically.
- **Virus –** A virus scanning service is installed on all devices and regularly monitored.
- **Backup** – Our storage is backed up on-site each day.

Third parties

- **Third party compliance** – We ensure third parties we contract with to store personal data comply with the principles of this policy, have an information security policy in place and ideally hold an information security standard (such as ISO 27001).
- **Limiting exports** – When exporting data from third party systems we only export the data we need for the purpose we need it for.
- **Google Docs (including Google Forms)** – We do not use Google Docs or Forms for the collation of personal information due to the data and forms collected being stored on users personal storage. If we need to use this functionality, we use Microsoft Forms (as part of our Office365 offering).

Consent

Where we do not have a lawful basis to hold or process data, we will seek the express consent of individuals to hold data about them. This will be by specific and unambiguous statements that must be opted-into on any forms (electronic or otherwise) and systems. In some circumstances we ask our members to ensure they have express consent for the data they are submitting to us.

Data Subject Access Requests

Should a member of the public request a copy of any personal information which Shapa holds, then the following process should be followed:

- The individual should write to the General Secretary(info@shapa.co.uk) outlining the personal data they are seeking to obtain.
- The General Secretary shall acknowledge the request by email.

- The General Secretary shall seek to verify the identity of the individual and that they are lawfully entitled to request a copy of the personal data. This may involve asking for information such as a membership number, date of birth, address, or documentary evidence.
- The General Secretary will collate the data requested, noting that we cannot provide data held by other organisations. The data should be carefully analysed to ensure it does not refer to any other individuals, in which case it should be redacted.
- Within 30 days of the receiving the request, the General Secretary will provide the data to the individual. This will normally be by email. There will be no charge.

For more information about our legal obligations, refer to the ICO website.

Right to erasure (Right to be forgotten)

Should a member of SHAPA or a member of the public wish for their personal information to be erased, then the following process should be followed:

- The individual should write to the General Secretary(info@shapa.co.uk) outlining the personal data they are seeking to erase.
- The General Secretary shall consult the Chair to make a decision as to whether the request should be processed. Guidance from the ICO should be followed. Whilst Shapa will not seek to refuse the request unreasonably, it has a number of statutory obligations to comply with and uses personal data as part of its vetting and safeguarding procedures.
- If it is deemed that the data shall be deleted, then the General Secretary will confirm to the individual the timescales involved and instruct the necessary responsible officer to delete it.

Correcting inaccurate personal data

Should a member of Shapa or a member of the public believe that information that we hold about them is inaccurate, they should write to the General Secretary(info@shapa.co.uk) outlining the inaccuracy. The General Secretary will then seek to correct the data and confirm back to the individual.

Reporting a breach

A breach is defined as any event which “leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”. If a breach occurs, the General Secretaryshould be immediately informed

The General Secretary (in consultation with the Chair) will need to consider if the breach is likely to “result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage”. If it does, the ICO should be informed within 72 hours of the breach occurring.

If the breach results in a high risk to the rights of the individuals involved, they should also be informed directly.