The Association of Early Pregnancy Units

DATA PROTECTION PRIVACY POLICY

ABOUT THIS POLICY

This Data Protection and IT Security policy applies to all operations of The Association of Early Pregnancy Units (AEPU. The policy is designed to ensure that the AEPU complies with its obligations under General Data Protection Regulation (GDPR) 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 AEPU Secretary is the owner of this policy and responsible for its annual review and update as necessary. The AEPU Secretary acts as our Data Protection Officer.

THE PERSONAL DATA WE HOLD

Data description	Personal data included	Stored using	Retention policy	Responsible officer
Information about our members	Contact information *(Includes sensitive data, as defined)*	Excel spreadsheet stored on Dropbox	6 months following ceasing to be a member to allow for variance in booking timescales for the annual conference	AEPU Secretary
Information about our conference delegates	Contact details, including name of hospital and job title *(Includes sensitive data, as defined)*	Event booking system managed by third party organiser and copies being transferred to AEPU in excel spreadsheet format stored on Dropbox	5 years following attendance to ensure data is held should delegates be questioned to provide evidence about CPD points	AEPU Secretary
Information about our employees or contractors	Applications where candidate/ company is unsuccessful	AEPU email	6 months after notifying candidate/ company to allow time for any questions regarding the selection process to be raised	AEPU Secretary
	Contact details start dates, annual leave, TOIL, contract, references, copy of other relevant documentation (e.g. disciplinary letters) *(Includes sensitive data, as defined)*	Dropbox for electronic copies. Secure storage at the home residence of the AEPU Chair for hard copies	5 years following the employee leaving employment or contract ceasing. Allows for references and retained information in the event of potential litigation	AEPU Chair
	Contact details, salary and pension contribution information	Not currently applicable	Indefinitely	AEPU Treasurer
	Copies of right to work checks, certificates and other physical documentation	Employment files stored at the home residence of the AEPU Chair for hard copies	5 years following the employee leaving employment/ cessation of	AEPU Chair

	provided by employees or contractors		contract. Allows for references and retained information in the event of potential litigation	
	Payroll information, including salary and other allowances, P60, P45, P11D and P6 notices.	Not currently applicable	7 years	AEPU Treasurer
Information about general enquirers	Contact information and nature of enquiry, which may contain personal data	AEPU email system	3 years in case of follow up questions	AEPU Administrator
Information about complainants	Contact information and nature of complaint, which may contain personal data	AEPU email system	3 years in case of follow up questions	AEPU Secretary
Information about people registered for our website	Contact information and which hospital they belong to	Wordpress	Indefinitely, unless the individual requests removal	AEPU Secretary
Information about people registered to our mailing lists	Contact information	Mailchimp (3rd party system)	Indefinitely, unless the individual chooses to opt out	AEPU Administrator

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	AEPU Treasurer
Finance – Receipt cash book and sales ledger	10 years	AEPU Treasurer
Trustee's minutes	Indefinitely	AEPU Secretary

Annual accounts and annual reports	Indefinitely	AEPU Secretary
Insurance policies	Indefinitely	AEPU Secretary
Employer's Liability insurance certificate	40 years	AEPU Secretary
Health and safety records	3 years	AEPU Secretary
Contract with customers, suppliers or agents, licensing agreements, rental/ hire purchase agreements, indemnities and guarantees and other agreements or contracts	5 years are expiry or termination	AEPU 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.
- **Passwords** – We use passwords either changed regularly or set once and keep until you think the password has been compromised.
- **Commercially available software** – where possible we use third party software to store personal data, such as Dropbox, where the software is regularly testing and patched for security vulnerabilities.
- **Employment** – We ensure our employees and contractors are made aware of their data protection obligations.
- **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.
- **Locked** – Physical documents with personal data will be stored in a locked cabinet.

Staff/Volunteer equipment

- **Virus –** A virus scanning service must be installed on all devices and regularly checked.
- **Removable storage –** Removal devices that will contain personal data should be encrypted using Bitlocker or similar encryption.

Staff/Volunteer emails

- **Restriction** - Our volunteers should always use the AEPU secure email system for receiving, storing and sending of emails when transmitting personal data.
- **Virus, Malware and Phishing protection** – All emails will be scanned for virus, malware and phishing.
- **IT security -** We rely upon the IT security provisions of Office 365 to provide an adequate level of security for our needs.

Third parties

- **Third party processing** – Other than the conference organiser, we limit the use of third parties to process personal data collected by the AEPU and only do so where we have the express permission of the AEPU Chair.
- **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).

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 due to the organisation of the AEPU, 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 AEPU or a member of the public request a copy of any personal information which the AEPU holds, then the following process should be followed:

- The individual should write to the AEPU Secretary (secretary@aepu.org.uk) outlining the personal data they are seeking to obtain.
- The AEPU Secretary shall acknowledge the request by email.
- The AEPU 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 AEPU 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 AEPU 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 the AEPU 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 AEPU Secretary (secretary@durhamscouts.org.uk) outlining the personal data they are seeking to erase.
- The AEPU Secretary shall consult the AEPU Chair to make a decision as to whether the request should be processed. Guidance from the ICO should be followed.
- If it is deemed that the data shall be deleted, then the AEPU 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 the AEPU or a member of the public believe that information that we hold about them is inaccurate, they should write to the AEPU Secretary (secretary@aepu.org.uk) outlining the inaccuracy. The AEPU 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 AEPU Secretary and AEPU Chair should be immediately informed (secretary@aepu.org.uk).

The AEPU Secretary (in consultation with the AEPU 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.

AEPU Website

The AEPU shares a summary about the data it holds and how it processes it on its AEPU website at https://www.aepu.org.uk/data-protection/. The website also provides information on how to submit a data subject access request and right to be forgotten request.