SEEAWA Data Protection Policy

Southeast & East Asian Women's Association (SEEAWA) • CIO No. 1203182

Version 2.1 • Updated with trustee approval, retention notes & cookie annex — 4 October 2025

Prepared by	Operations & Systems Manager
Data Protection Lead	Sarah Reid — Advocacy and Policy Manager (sarahreid@seeawa.org.uk)
Designated Digital Safeguarding Officer (DDSO)	Sarah Reid — Advocacy and Policy Manager
Trustee Champion	Susan Cueva
Date of approval	October 2025
Next review	October 2026 (or sooner if guidance changes)
Scope	Staff, volunteers, trustees, contractors, service users

Contents

• Annex A — Retention Schedule (summary)

1. Purpose & Scope

This Policy sets out how **SEEAWA protects personal data and upholds the rights of individuals. It applies to all personal data we process, in any format (digital or paper), across all activities and systems we use.**

2. Legal Framework (as of October 2025)

• UK GDPR and Data Protection Act 2018 (DPA 2018).

• Privacy and Electronic Communications Regulations (PECR).

• Data (Use and Access) Act 2025 (DUAA) — amends UK GDPR/DPA/PECR; staged commencement in 2025–2026.

• Relevant ICO guidance, codes and sector standards (e.g., Caldicott for health/social care).

Monitoring changes

• We track DUAA commencement regulations and ICO guidance; we will update notices and processes when measures take effect.

3. Roles & Responsibilities

• **Trustees** — accountable for data protection and risk oversight; approve this Policy.

• **Data Protection Lead** — Sarah Reid: oversee compliance, DPIAs, DSARs, breaches, training, and liaison with the ICO.

• **Managers** — implement controls in their teams; ensure processors meet our standards.

• **All staff/volunteers** — handle data lawfully; complete training; report incidents promptly.

4. Data Protection Principles

• Lawfulness, fairness, transparency — be clear and have a lawful basis.

• Purpose limitation — collect for specified, explicit, legitimate purposes.

• Data minimisation — only what is necessary.

• Accuracy — keep information up to date.

• Storage limitation — don't keep data longer than necessary (see Annex A).

• Integrity & confidentiality — protect with appropriate security.

• Accountability — document decisions and controls.

5. Lawful Bases (incl. Recognised Legitimate Interests)

We use one of the lawful bases under Article 6 UK GDPR for each processing activity. **These include consent, contract, legal obligation, vital interests, public task (where applicable), and legitimate interests.**

Under the DUAA 2025, certain purposes may qualify as "recognised legitimate interests" (RLI). Where an RLI applies, we still apply a necessity test and safeguards, but a formal balancing test may not be required. Examples include:

• Network and information security; prevention/detection of fraud or crime.

• Safeguarding of children and individuals at risk.

• Direct marketing by the data controller (respecting PECR and the right to object).

We document the lawful basis (and Article 9 condition where relevant) in our Record of Processing Activities (ROPA) and Privacy Notices.

6. Special Category & Criminal-Offence Data

Where we process special category data (e.g., health, ethnicity) or criminal-offence data, we identify an Article 9 (and DPA Schedule 1) condition — commonly: explicit consent; vital interests; legal claims; safeguarding of children and individuals at risk; or employment/social protection. We put in place appropriate policy documents and access restrictions.

7. Transparency & Privacy Notices

We provide clear Privacy Notices at or before the point of collection (or within one month if obtained indirectly), explaining purposes, lawful basis, retention, sharing, international transfers, rights, and how to complain to the ICO.

8. Data Minimisation, Accuracy & Retention

- Collect the minimum necessary data; avoid fields we don't use.
- Review accuracy at key touchpoints (intake, referrals, case reviews).
- Apply retention from Annex A; set a deletion review task; pause deletion if a legal hold applies.

9. Individual Rights & Requests

- Right to be informed, access, rectification, erasure, restriction, portability, object, and rights re automated decision-making.
- We verify identity where needed and respond within one month (extend by two months for complex requests).
- We record decisions, exemptions relied on, and disclosures; we provide data in a commonly used format.

10. Security & Access Controls

- Role-based access

• Approved platforms and processor contracts; UK/EU data residency preferred or appropriate safeguards.

• Backups and secure configuration; patching; phishing awareness; safe BYOD rules.

• Incident detection and response processes; regular access reviews.

12. Governance, Training & Review

• Annual training for staff and regular volunteers; induction on start.

• Annual review of this Policy

• Complaints route: Data Protection Lead; escalate to ICO if unresolved.

Annex A — Retention Schedule (summary)

Record type	How long to keep	Clock starts	Notes	Funder/Insurer override?
Service user case files (adult)	7 years (20 years for serious incident/MARAC)	Case closure	Pause deletion on legal hold.	Yes — follow funder/insurer if longer
Safeguarding logs (index)	10 years	Year-end	Audit & pattern analysis.	
HR/volunteer personnel files	6 years after leaving	Leaving date	H&S incidents may require longer.	Yes —
Recruitment records (unsuccessful)	6 months	Decision date	Extend if complaint/claim raised.	As required
DBS certificate copy	Max 6 months	Decision date	Outcome metadata: 6 years.	No (DBS Code)
Training records	6 years after leaving	Leaving date	Proof of compliance.	As required
Financial records (invoices, receipts)	6 years	Financial year-end	Per HMRC rules; 10 years for VAT in some cases.	Yes — per HMRC/contract
Grants/contracts deliverables	7–10 years	Contract end	Per contract or funder guidance.	Yes — follow contract

Note: This schedule represents SEEAWA's default minimum retention. If a **legal hold**, regulator request, insurance matter, or funder contract applies, suspend deletion and retain as required. Record the hold and review quarterly.

The **ICO** is the UK's **Information Commissioner's Office** — the independent regulator for information rights. It:

- **Enforces UK data laws**: UK GDPR, Data Protection Act 2018, PECR (e-privacy/cookies), Freedom of Information, and more.
- **Guides and supervises**: publishes practical guidance and statutory codes (e.g., **Data Sharing Code**, **Children's Code**).
- **Investigates & fines**: can audit, issue enforcement notices, and fine up to **£17.5m or 4%** of global annual turnover for the most serious breaches.
- **Handles complaints** from the public about misuse of data or access requests.

What this means for SEEAWA

- **Report data breaches** to the ICO within **72 hours** if they pose a risk to people's rights and freedoms.
- **Pay the data protection fee** (most UK controllers must) and keep your details up to date.

Approved:

Trustee Champion:

Susan Cueva