SEEAWA Digital Safeguarding Policy and Procedure

Southeast & East Asian Women's Association (SEEAWA) • CIO No. 1203182 *Version 2.0* • *Updated to UK law as at 4 October 2025*

Prepared by:	Operations & Systems Manager
Designated Digital Safeguarding Officer (DDSO)	Sarah Reid — Advocacy and Policy Manager
Trustee Safeguarding Champion	Susan Cueva
Approved by Trustees	Dec 2025
Review cycle	Annual — Next review Oct 2026 (or sooner if guidance changes)

1. Purpose & Scope

This Policy sets out SEEAWA's standards and procedures to safeguard staff, volunteers, service users and partners in **digital contexts (online platforms, messaging, video-conferencing, email, social media, websites, and digital events).** It applies to all **staff, trustees, volunteers, contractors and partners** who act on behalf of SEEAWA, and to any digital channels or systems used for SEEAWA work—whether organisation-managed or personal devices ('BYOD') used for work.

SEEAWA primarily supports adult women and their children from Southeast and East Asian communities, including survivors of domestic abuse, modern slavery and trafficking. Where activities involve or may reach under-18s, this Policy must be read alongside local safeguarding arrangements and school/college policies.

2. Legal & Policy Framework (as of 4 October 2025)

This Policy aligns with current UK law and official guidance, including (non-exhaustive):

• Online Safety Act 2023 (OSA) — including Part 10 communications offences and Ofcom online-safety regime.

• OSA offences in force (2024–2025): encouraging/assisting serious self-harm; cyberflashing; false/threatening communications; epilepsy-trolling; intimate-image abuse (incl. deepfakes).

• Sexual Offences Act 2003 (as amended) — incl. s.66A cyberflashing.

• New offence (2025): creating sexually explicit 'deepfake' images without consent. SEEAWA Digital

• Data (Use and Access) Act 2025 — updates to UK data law; ICO guidance under review.

• UK GDPR & Data Protection Act 2018; PECR.

• Prevent duty guidance (Home Office) — with local Channel/MASH routes. • If working with schools/under-18s: Keeping Children Safe in Education (KCSIE) 2025.

We will monitor updates

- Track Ofcom, CPS and ICO guidance changes and update procedures.
- Review this Policy sooner if legal or regulatory changes occur.

3. Roles & Responsibilities

Board of Trustees — provide strategic oversight; approve this Policy; ensure resources for implementation, training and incident management.

Trustee Safeguarding Champion — governance challenge and assurance that safeguarding (including digital) is embedded across SEEAWA.

Designated Digital Safeguarding Officer (DDSO): **Sarah Reid** — Advocacy and Policy Manager — leads digital safeguarding: advice, triage, referrals, liaison with authorities/platforms; maintains incident log; oversees training and annual review. First point of contact for concerns.

Managers & Circle Leads — ensure team compliance; complete risk assessments; ensure contractors/practitioners adhere to this Policy and codes of conduct.
All staff, volunteers and contractors — follow this Policy and complete required training; use only authorised tools; report all concerns immediately.
Digital safeguarding covers harm arising via digital systems or platforms**: abuse, harassment, grooming, coercive control, stalking, doxxing, hate incidents, threats, scams, impersonation, non-consensual imagery, and harmful misinformation.**

4. Definitions & Online Harms

Specific criminal harms (non-exhaustive):

- Cyberflashing (SOA
- False communications and threatening communications (OSA 2023 Part 10). • Epilepsy-trolling (malicious flashing images) (OSA 2023).
- Encouraging/assisting serious self-harm (OSA 2023).
- Intimate-image abuse incl. creation/sharing or threats to share, including deepfakes (2025 offence).
- Voyeurism/down-blousing/up-skirting; sexual communication offences. • Stalking and harassment; malicious communications; hate crime; doxxing. • CSAM/grooming (report to police/CEOP/IWF).

Evidence handling

• Do not forward/store illegal content.

• Capture URLs/handles and timestamps; take a screenshot only if safe and lawful.

• Escalate immediately to DDSO; consider police/CEOP/IWF/Report Harmful Content and platform reporting.

5. Behaviour & Safe Practice

Professional boundaries online — Use work accounts for work; keep communications professional; avoid personal friend/follow with service users; avoid one-to-one messaging out of hours unless risk-related and recorded.

Contact methods — Prefer SEEAWA email/CRM/approved messaging; if you must use a personal device in exigencies, record the interaction in SEEAWA systems promptly.

Recording & images — Obtain informed consent before recording or sharing images; comply with storage/retention rules and platform terms.

Moderation & events — For online groups/events, appoint a moderator; use waiting rooms; disable private chat where needed; publish ground rules; debrief after incidents.

6. Reporting & Responding to Concerns

Report any concern immediately to the DDSO (or deputy). Where there is immediate danger, call 999.

- **Preserve** evidence; **do not forward illegal content**.
- Log the incident in the safeguarding record **within 24 hours**.
- DDSO assesses risk and decides on referrals (police, CEOP, IWF, MASH/Channel, platform reporting), **informing the Trustee Champion as appropriate.**
- **Support the affected individual(s);** agree safety steps (privacy settings, device safety, safety planning).
- **Record outcomes and lessons learned;** update risk assessments.

External reporting links:

- **Police (999/101).**
- **Report Harmful Content (reportharmfulcontent.com).**
- **CEOP (child exploitation/online grooming).**
- **Internet Watch Foundation (CSAM).**
- **Platform in-app reporting tools (per Ofcom guidance).**
- **Local MASH / Channel (radicalisation concerns).**

7. Data Protection & Privacy

SEEAWA processes personal data in line with UK GDPR, DPA 2018, PECR and the Data (Use and Access) Act 2025. We follow the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality and accountability.

Operational controls:

• DPIAs for high-risk digital activities (online groups, recordings, new apps).

Do a simple **Data Protection Impact Assessment** (privacy risk check) before you run things like **online support groups**, **recordings**, or adopt **new apps**.
Example: Before hosting a Zoom circle you'll record, complete a 1-page DPIA: what data you'll collect, risks (e.g., accidental disclosure), and how you'll reduce them (waiting room, no names on screen, secure storage).

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

Use tools that have proper **data-processing terms** and strong security. Prefer services that store data in the **UK/EU** (or have strong legal safeguards if not).
Example: Keep a "**Approved Tools List**" (e.g., Microsoft 365, Google Workspace, Zoom) and file the vendor's **Data Processing Agreement**.

• Strong authentication; role-based access; avoid shared accounts; encryption where available.

Turn on **2-step verification (2FA)**; give people the **minimum access** they need; don't share logins; use **encryption** (in transit and at rest) whenever possible.
Example: Everyone uses their own account with 2FA; only the DDSO and relevant staff can open safeguarding folders.

• Retention per schedule; restrict safeguarding records to DDSO/need-to-know.

Keep records only for as long as your **Retention Schedule** says, then securely delete.
Limit access to the **DDSO and essential staff**.
Example: Safeguarding case notes kept for the set number of years, stored in a restricted folder, auto-reviewed for deletion.

Children's Code standards where services could be accessed by children.

If anything you do **might reach under-18s**, follow the ICO's **Age-Appropriate Design Code**: high privacy by default, minimal data, clear notices, no unnecessary tracking. *Example:* If you host a public live stream, turn off analytics/trackers you don't need and avoid collecting names/contacts from minors.

• Review privacy notices and lawful-basis assessments as ICO guidance updates under DUAA.

When the regulator updates guidance, **refresh your Privacy Notice** and check your **lawful basis** for processing (e.g., consent, legitimate interests, vital interests). *Example:* If you start recording sessions for training, update the Privacy Notice to say what's recorded, why, how long you keep it, and who can see it.

8. Devices & Secure Working

Prefer **SEEAWA-managed devices**. For BYOD, apply mobile-device security (screen-lock, auto-update, anti-malware, encryption where available). **Do not store case data unencrypted.** Use password managers and 2FA.

Public Wi-Fi — avoid accessing sensitive data on unsecured networks; use a VPN where appropriate.

9. Digital Risk Assessment

Before launching **new digital channels or events**, complete a **risk assessment** covering **platform settings, moderation, participant safety, consent, data flows, and incident response**. Re-assess after incidents or major changes.

10. Training & Induction

All staff and regular volunteers complete induction training on this Policy and annual refreshers. **If you work with schools or under-18s, match the schools' rhythm.** KCSIE (Keeping Children Safe in Education) expects **annual** safeguarding training **plus in-year updates** when guidance changes. So any SEEAWA team delivering in/with schools should do: (1) a yearly session and (2) bite-size updates when there's new guidance (e.g., a 15-minute briefing or PDF summary).

Track completion so you can prove compliance.
Keep a simple log that shows who did what, when. Auditors/funders will oftenask.

11. Safer Recruitment & DBS

Roles with digital contact or access to sensitive systems are risk-assessed for **DBS level and supervision**. Contractors/practitioners engaged for digital services must agree to this Policy and code of conduct.

12. Complaints & Whistleblowing

Concerns about digital safeguarding practice can be raised through **SEEAWA's Complaints Policy or Whistleblowing Policy**. The **DDSO/Trustee Champion** will ensure concerns are investigated promptly and fairly.

13. Governance & Review

This Policy is **prepared by the Operations & Systems Manager and the DDSO.** It is reviewed annually by the Trustee Safeguarding Champion (or sooner if law/guidance changes), approved by the Board, and published to staff/volunteers.

14. Safeguarding Procedures

Southeast and East Asian Women's Association (SEEAWA) Policy Document – Safeguarding Vulnerable Adults Policy and Procedure

Safeguarding Procedures:

It is the responsibility of everyone working on behalf of SEEAWA (staff/volunteers), to understand SEEAWA's Safeguarding policy & procedures.

To achieve good practice in our setting we will ensure the following areas are clear and put into practice:

1) Safer Recruitment & Selection

All staff/volunteers will go through the following process prior to delivering/ supporting activities/services to vulnerable adults.

We have a policy and procedure which ensures that all paid staff and volunteers:

- Complete an application form or a letter of application. This includes: **address, evidence of relevant qualifications, the reasons why they want to work with vulnerable adults, paid work and voluntary work experience and all criminal convictions.**
- Provide **two pieces of identification** which confirm both **identity and address**.
- Undergo an interview (formal or informal) involving at least **two interviewers.**
- Provide at least **two references** which are followed up before a post is offered. One reference is from the last employer or an organisation that has knowledge of the applicant's work or volunteering with vulnerable adults. If the applicant has not worked with vulnerable adults before, then they should confirm this and give an

alternative referee.

- **Consent to a Disclosure and Barring Service check** (formal CRB check) at the appropriate level (standard or enhanced). Agree to sign up to the DBS update service.

Furthermore, the organisation complies with all other safeguarding regulations:

- We understand that a person who is barred from working with vulnerable adults is breaking the law if they work, volunteer, or try to work or volunteer with these groups.

- We understand that an organisation which knowingly employs someone who is barred to work with those groups will also be breaking the law.

- We understand that if our organisation dismisses a member of staff or volunteer because they have harmed a vulnerable adult, or would have done so if they had not left, we must complete a DBS referral form.

- SEEAWA will have an induction process including access to policies, procedures and code of conduct expected to be followed by all those delivering services on behalf of SEEAWA to support their work.

- An appraisal system in place to identify any concerns or issues.

2) Management & Support of Paid Staff & Volunteers

- All staff and volunteers will be provided with a job description (paid staff) or a **role profile (volunteers)** outlining their main responsibilities. This includes a requirement to comply with our **Safeguarding Policy and procedures and ground rules for appropriate behaviour.**

- All staff and volunteers are supported through an induction process in which safeguarding procedures are explained and training needs identified.

- All paid staff and volunteers complete a role review at the end of their induction period before being confirmed in post. Inductions will be completed within 6 months.

- All paid staff are given supervision at least every 8 weeks by the designated authorised person of the organisation.

- All volunteers are given regular support sessions. (This may include one to one or group support, mentoring or shadowing opportunities).

- Implements disciplinary and grievance procedures for all paid staff and volunteers.

- All paid staff and volunteers attend regular ongoing safeguarding training appropriate to their role.

- All paid staff and volunteers receive an induction, which includes information on all the organisation's policies and procedures.

3) Safer working practice:

We will ensure that adequate staff and/or volunteers are supporting activities that SEEAWA runs.

All activities are properly planned and organised. Planning ensures that the activities are age- appropriate, appropriately supervised, take staff ratios into account and use qualified instructors.

- Risk Assessments for activities are carried out prior to delivering activity sessions.
- All activities are risk assessed to ensure that all reasonable steps are taken to prevent vulnerable adults being harmed whilst participating in the organisation's activities.

- We will regularly assess and review safety risks which arise from premises, activities, equipment and travel arrangements, as outlined in the organisation's Health and Safety Policy.

- Ground rules are set for appropriate behaviour for vulnerable adults, staff, volunteers, parents and carers. Systems are in place and implemented if the ground rules are broken.

- We will ensure that images of vulnerable adults and families are only used after written permission has been obtained, and only for the purpose for which consent has been given.

4) Providing Safer Activities and Trips

Necessary arrangements:

- People whose suitability has not been checked, including through a DBS check, must not be allowed to have unsupervised contact with vulnerable adults.

- All paid staff and volunteers undertaking specialist roles are provided with appropriate training.

- Employer liability and/or public liability insurance has been taken out to ensure that all activities and services and all people taking part, are covered.

5) Responding to concerns

If any member of staff/volunteer is concerned about an adult at risk, they must inform the nominated safeguarding lead person (NSP) or deputy NSP immediately.

- The written record must be clear, precise and a factual account of observations or what has been said.
- The NSP will decide on the most appropriate course of action and whether the concerns should be referred to other social service providers. If it is decided that a referral needs to be made, this will be discussed with the adult at risk. All concerns, discussions and decisions will be recorded in writing.
- If a member of staff disagrees with the level of concern and feels that an adult at risk has not been protected, then any member of staff can make a direct referral.

Disclosure by a Vulnerable Adult:

SEEAWA recognises that an adult at risk may seek you out to share information about abuse or neglect, or talk spontaneously, individually or in groups when you are present. In these situations, YOU MUST:

- Listen carefully to the vulnerable adult. You can seek clarification but DO NOT ask direct questions or start to investigate the matter.
- Give the adult at risk time and your full attention.
- Allow the adult at risk to give their account; do not stop an adult at risk who is freely recalling significant events.
- Make an accurate record of the information you have been given, taking care to record the timing, setting and people present. Make a record of the adult at risk's presentation as well as what was said. Do not throw this away as it may later be needed as evidence.
- Use the adult at risk's own words where possible.
- Explain that you cannot promise not to speak to others about the information they have shared - do not offer false confidentiality.

Reassure the Vulnerable Adult that:

- They have done the right thing in telling you.
- They have not done anything wrong.

- Tell the adult at risk what you are going to do next and explain that you will need to get help to keep him/her safe.

- DO NOT ask the adult at risk to repeat her account of events to anyone. ● You must log and record information regarding concerns on the same day.

Allegations Against Adults Who Work with Vulnerable Adults

If you have information which suggests an adult who works with vulnerable adults (in a paid or unpaid capacity) has:

- Behaved in a way that has harmed or may have harmed a vulnerable adult. ● Possibly committed a criminal offence against, or related to, a vulnerable adult.
- Behaved towards a vulnerable adult in a way that indicated s/he is unsuitable to work with vulnerable adults.

You should speak immediately with the Nominated Safeguarding Lead Person (NSP) or your manager who has responsibility for managing allegations. The NSP will consult with/make a referral to the LADO (Local Authority Designated Officer) via the MASH (Multi-agency Safeguarding Hub) Team. If one of those people is implicated in the concerns you should discuss your concerns directly with the LADO (Local Authority Designated Officer) via the MASH Team.

Making a Referral

A referral will involve providing information of concern to the Nominated Safeguarding Lead Person (NSP) (unless the concern is about the Nominated Safeguarding Person) about an Allegation against a staff/ volunteer.

The MASH will need to be contacted in order for the Local Authority Designated Officer (LADO) to be informed. The LADO will make enquiries and take appropriate action, provide guidance and may request for further information to be submitted.

You may be called for a meeting with the LADO. The LADO may have to speak to the Police to decide if a criminal act has taken place, in serious cases the Police may be informed and may investigate.

You will be informed of the action that will be taken by the LADO.

YOU SHOULD NOT:

- Call a staff meeting and discuss the matter with staff/volunteers. The LADO will guide you on what needs to be done.

- You should not try and bring the perpetrator of the alleged abuse in contact with the victim to discuss concerns.

- Do not delay your response.

There are some cases that require an urgent response. If a vulnerable adult is in immediate danger or is at harm or risk you should refer to the social care and/or the police.

If you suspect a serious criminal act has taken place, telephone 999. Tell them if you think it might be adult abuse. If the individual is injured, seek immediate medical treatment. Tell the ambulance personnel or A&E staff that this is a potential adult abuse situation.

- In emergency dial 999
- Multi-Agency Safeguarding Hub (MASH):

Email: enquiry@towerhamletsconnect.org

Tel: 0300 303 6070 (weekdays 9am to 5pm)

We recommend also emailing a **safeguarding alert form** to **enquiry@towerhamletsconnect.org**.

Tower Hamlets Connect staff will send this directly to the local authority/initial assessment team.

Out of hours emergency duty team:

Tel: 020 7364 4079 (5pm to 9am including weekends).

https://www.towerhamlets.gov.uk/lgnl/community_and_living/community_safety__crime_preve/domestic_violence/Domestic-abuse.aspx

Action To Be Taken Following the Referral:

SEEAWA will ensure that you keep an accurate record of your concern(s) made at the time. SEEAWA puts concerns in writing to the social care team following the referral within 48 hours duty.

SEEAWA will accurately record the action agreed or that no further action is to be taken and the reasons for this decision.

Confidentiality

SEEAWA will ensure that any records made in relation to a referral are kept confidentially and in a secure place. Information in relation to adult safeguarding concerns should be shared on a "need to know" basis. **Note**: The sharing of information is vital to adult protection and, therefore, the issue of confidentiality is secondary to the need for protection.

Challenges & Escalation
All staff and volunteers need to be robust in constructively challenging colleagues, when necessary, to achieve the best outcome for vulnerable people.

Whistle Blowing

This is the confidential disclosure by any individual of any concern encountered in the workplace related to a perceived wrongdoing. SEEAWA considers such

wrongdoing to include:

- General malpractice, such as immoral, illegal or unethical conduct •

  Conduct where someone's health and safety has been put in danger. •

  Gross misconduct.

If individuals have concerns relating to their employment with SEEAWA these should be raised under SEEAWA's grievance policy. Where it is felt that the organisation has not or will not address the concerns appropriately, there are several services available:

- Whistleblowers UK - https://www.wbuk.org/help
- Care Quality Commission - 03000 616 161
- Action on elder abuse 0808 808 8141 – (Hourglass)
- If there is immediate danger, call 999.

• Report to DDSO — Sarah Reid (Advocacy and Policy Manager)

sarahreid@seeawa.org.uk.

• Record the incident in the safeguarding log within 24 hours.

• Preserve evidence (URLs/handles, timestamps); do not forward illegal

• Refer to Police/CEOP/IWF/Report Harmful Content/MASH-Channel as applicable.

• Support the person affected; review privacy/device safety; debrief with manager/DDSO; update risk assessment.

• Platform choice (moderation tools; waiting rooms; recordings off by default).

Pick a video/app that gives the host control: waiting room, mute-all, remove/block, disable private chat/file-sharing, spotlight, captions. Set **recording = off by default** so nothing is captured unless you've got consent and a plan.
Example: Zoom with Waiting Room on, Only host can share screen, Private chat off, Recording disabled.

• Access control (registration; joining instructions; code of conduct).

Control who can get in and how they behave. Use a simple registration list (first name/initials is fine), send **joining instructions** (link + start time + who to contact), and include a short **code of conduct** (confidentiality, respectful chat, camera optional, how to report concerns).
Example: Don't post links publicly; use unique meeting IDs and a

passcode. **• Consent (recording/photography; opt-out mechanics;**

retention).

If you want to **record** or take screenshots, **ask first** and explain why, who sees it, where it's stored, and **how long** you'll keep it. Give an **opt-out** (camera off, use initials, be placed in a non-recorded breakout, or note-taking instead of recording).
Example: "We're not recording. If this changes, we'll ask your consent and you can opt out."

• Moderation (assigned moderator; escalation script; back-channel).

Name a **moderator** (not the facilitator) to watch chat, admit people, mute/remove if needed, and capture safeguarding concerns. Prepare a short **escalation script** ("I'm going to pause, remove the disruptive participant, and we'll resume in one minute") and a **back-channel** (DM/WhatsApp) between host/mod.
Example: Moderator has pre-typed messages for ground rules and for pausing the

session. **• Data flows (storage location; processors; transfers).**

Know **where data goes**: registration list (e.g., Eventbrite/Google Form) → video platform (Zoom/Teams) → any files/recordings (OneDrive/Drive). Make sure each tool is **approved**, has a **data-processing agreement**, and—ideally—UK/EU data residency or proper safeguards. Keep only what you need.
Example: Registration in Google Form (UK/EU data centres if available) → attendance note in Microsoft 365 → no recordings saved.

• **Aftercare (sign-posting; follow-up; incident logging).**

Plan what happens **after** the event: send **support sign-posts** (helplines, SEEAWA contact), check in with anyone who seemed distressed, and **log any incidents** (what happened, action taken, outcome). Do a quick team **debrief** and update your risk assessment if needed. *Example:* Follow-up email: "Thanks for joining—here are resources and our safeguarding contact. Tell us privately if you need support."

This policy and procedure document should be used in conjunction with:

- Ending Violence Against Women & Girls (VAWG) Policy,
- Health & Safety Policy,
- Equality, Diversity, and Inclusion Policy and
- Data Protection Policy.

Approved by Trustee Champion:

Trustee

Susan Cueva