

Privacy Notice

Version 2.0

Public Privacy Notice

Document owner	Chief of Staff
Approved by	Chief Executive Officer
Effective date	10 September 2026
Review date	September 2027, or earlier following a material change

1. About this notice

The Security Institute (the “Institute”, “we”, “us” or “our”) respects your privacy and is committed to protecting your personal information. This Privacy Notice explains how we collect, use, store and share personal information, the lawful bases on which we rely, and the rights available to you under UK data protection law.

This notice applies to members, applicants, former members, event attendees, volunteers, speakers, contributors, website and application users, professional partners, suppliers, contacts and other individuals who interact with the Institute. We may provide additional privacy information for a particular activity where needed. Our separate Cookie Notice explains our use of cookies and similar technologies.

2. Who we are

The Security Institute is the data controller responsible for the personal information described in this notice.

Legal name	The Security Institute
Registered address	1 Witherley House, Hazell Way, Nuneaton, Warwickshire, England, CV10 7PQ
Company details	Company number 03961350. Private company limited by guarantee, registered in England and Wales.
Data Protection Lead	Vikki Fox, Chief of Staff
Email	Vikki@security-institute.org
Telephone	02476 346 464

3. What personal information we collect

The information we collect depends on your relationship with us and the services or activities in which you participate. It may include:

- identity and contact information, including name, title, preferred name, date of birth, address, email and telephone details;
- membership information, including membership number, grade, status, application, validation, reference, vetting, revalidation and membership history;
- payment, subscription, event and transaction records;
- professional information, including job title, employer, sector, role, career background, security experience, specialisms, qualifications, accreditations and CPD;
- event, learning and engagement information, including bookings, attendance, participation, dietary/accessibility requirements, mentoring, volunteering and feedback;
- communications and preference information, including service messages, marketing choices and consent records;
- digital information, including website/portal/app use, device/browser, login, audit and security information; and
- photographs, biographies, publications or other content you provide or that is created in connection with Institute activities.

4. Enhanced member profile information

We invite members to provide additional profile information through the Members' Portal so that we can understand the membership and profession we represent and improve the relevance of our services. This may include employment sector, role, career stage, previous career background, security specialisms, qualifications, professional interests, development aspirations, volunteering interests and preferred content or engagement formats.

Some information is required to administer membership or provide a requested service. If you do not provide information that is required for an application, validation or membership service, we may be unable to process your application or provide the relevant service. Other profile information is optional. Where disclosure is optional, you may decline to provide it or select options such as "Prefer not to say", "Not applicable", "None" or "Other" where available.

Members can update much of their own information through the Members' Portal. This helps improve accuracy and reduces the need to create additional personal information through emails or telephone notes.

5. Equality, diversity and inclusion information

We invite members to provide optional equality, diversity and inclusion (EDI) information so that we can understand representation within our membership, identify trends or areas of under-representation and improve our services and opportunities.

EDI questions may include gender, ethnicity, disability or health information and sexual orientation. Some of this is special category personal information under UK GDPR. Where we ask for special-category EDI information, we obtain your explicit consent before processing it. The consent is separate from your substantive EDI response, and you may choose "Prefer not to say" where offered.

Providing EDI information is voluntary and will not affect your membership, membership grade or access to services. You may withdraw your consent through the Members' Portal. Where consent is withdrawn, we stop the consent-based processing and apply our approved deletion or suppression process. EDI reporting will normally be aggregated or anonymised and controlled to reduce the risk of individuals being identified.

6. Children and young people

We may process personal information about children and young people through young-people events, outreach, education and early-career activities. Where we knowingly collect information about someone under 18, we provide age-appropriate information and apply safeguards appropriate to the activity and age of the participant.

Where a young person attends through a school, cadet force, youth organisation or other organised group, that organisation may provide registration or permission information to us and identify relevant restrictions. For photography and publication involving under-18s, we apply our Photography and Filming Procedure and obtain appropriate parent/guardian or organising-body confirmation where required.

7. How we collect personal information

We may collect personal information:

- directly from you when you apply for or renew membership, update your profile, register for an event, record CPD, contact us, volunteer or otherwise use our services;
- from an employer, university, training provider, corporate partner, event organiser, referee, sponsor or other person involved in a service or validation process;
- from service providers that operate systems or services on our behalf;
- from publicly available professional sources where necessary and proportionate, including limited use of LinkedIn or a previous employer to re-establish contact where our existing contact details no longer work; and
- automatically when you use our websites, portals, applications or online services.

8. Why we use personal information and our lawful bases

We use personal information only where we have a lawful basis. The basis depends on the activity and the information involved.

Purpose	Examples of information	Lawful basis
Membership and applications	Identity, contact, grade, validation and payment information	Contract; legal obligation for relevant accounting/statutory records
Membership vetting and relevant criminal-offence information	Vetting information and relevant declarations	Legitimate interests, with an applicable Schedule 1 Data Protection Act 2018 condition; consent where relied upon
Events, CPD and requested member services	Booking, participation, learning and service records	Contract; legitimate interests for volunteering/mentoring; explicit consent where optional special-category information is requested
Accurate records and member self-service	Contact and professional profile information	Legitimate interests
Understanding membership and improving services	Sector, career, specialism, qualification and engagement information	Legitimate interests
Optional special-category EDI	Ethnicity, disability/health,	Article 6 legitimate interests and Article

Purpose	Examples of information	Lawful basis
information	sexual orientation and other special-category EDI information	9(2)(a) explicit consent
Operational communications	Membership and contact information	Contract
Marketing and promotional communications	Contact details, preferences and relevant segmentation	Consent, with applicable PECR requirements
Website analytics and non-essential cookies	Cookie/online identifiers, device/browser and usage information	Consent
Finance, accounting and statutory compliance	Payment, transaction and governance records	Legal obligation
System security and incident management	Login, device, access, audit and incident information	Legitimate interests
Complaints and professional standards	Correspondence, evidence and decision records	Legitimate interests, with additional conditions where special-category or criminal-offence information is involved
Re-establishing contact	Existing member details and limited publicly available professional information	Legitimate interests

Where we rely on legitimate interests, we consider the purpose, necessity and impact on individuals and apply safeguards so that our interests are not overridden by your rights and freedoms. You may object to processing based on legitimate interests, although this right is not absolute.

9. Membership applications, validation and vetting

Applicants provide information such as an application form, CV, professional history, references and, where applicable, vetting or relevant criminal-offence information. We use this information to assess eligibility for membership and the appropriate professional grade.

A scoring-aligned summary of the information relevant to the membership criteria is created for the validation process. The Validation Board uses the summary and approved criteria to reach its decision. The Institute does not make the final membership or grade decision solely by automated means.

Where we process criminal-offence information as part of membership vetting, we identify an Article 6 lawful basis and an applicable condition under Schedule 1 of the Data Protection Act 2018. Where we rely on consent for this purpose, the consent is specific, informed and capable of withdrawal.

10. Communications, profiling and artificial intelligence

We distinguish between communications necessary to administer membership or provide a requested service and optional marketing or promotional communications. Marketing communications are sent in accordance with

applicable data protection and PECR requirements. You can manage applicable preferences through your profile or by using the unsubscribe mechanism in a communication, and you may ask us to stop direct marketing at any time.

We may use profile information to segment communications, identify relevant events or professional opportunities, understand membership trends and improve services. This may involve limited profiling but is not intended to produce legal or similarly significant effects.

We may use authorised artificial intelligence tools to support administrative tasks, drafting, summarisation, search, process improvement and controlled testing. Where personal information is involved, use is governed by our AI policies, approved-use register, data protection controls and human oversight. We do not use artificial intelligence to make final automated decisions about membership admission, grade, conduct, disciplinary matters or professional recognition.

We may also use anonymised or appropriately de-identified member and applicant information to test, benchmark and improve administrative processes, including tools that assist with summarisation, categorisation or workflow improvement. We use anonymised or synthetic information wherever this can reasonably achieve the testing purpose. Where information can still be linked back to an individual, we continue to treat it as personal information and apply appropriate security, data-minimisation and human-oversight controls.

11. Who we share personal information with

We share personal information only where necessary, proportionate and lawful. Recipients may include:

- technology providers supporting our CRM, website, Members' Portal, applications, community platform, email, finance, events and IT services;
- payment providers, banks, accountants, auditors and professional advisers;
- event venues, speakers, mentors, assessors, validation or professional-recognition participants where needed to provide a service;
- employers, universities, learning providers, corporate partners or other organisations where you request or authorise the interaction;
- regulators, law enforcement agencies, courts or public authorities where required or permitted by law; and
- other parties involved in a legal claim or organisational transfer, subject to appropriate safeguards.

We do not sell personal information. Suppliers acting as processors must use personal information only on our instructions and under appropriate contractual, confidentiality and security obligations.

12. International transfers

Some suppliers or support arrangements may involve personal information being stored in, accessed from or transferred to countries outside the United Kingdom. Where this occurs, we use a lawful transfer mechanism and appropriate safeguards, such as UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to approved standard contractual clauses, together with any required transfer-risk assessment.

More detailed information about international processing associated with cookies and analytics is provided in our Cookie Notice.

13. How long we keep personal information

We keep personal information only for as long as reasonably required for the purpose for which it was collected, including legal, accounting, regulatory, professional-standards, dispute-resolution and safeguarding requirements. When information is no longer required, it is securely deleted, destroyed or anonymised in accordance with our Corporate Records Retention Schedule.

- Core member information is retained throughout active membership and for 3 years after cancellation. Where the member is aged 21 or under at cancellation, the post-cancellation period is 12 months, unless a specific legal, safeguarding or professional-record requirement applies.
- For successful membership applications, the application/CV, supporting evidence, vetting information and referee data are normally deleted 3 months after successful joining/final validation. The final scoring-aligned validation summary, decision and grade are retained as part of the membership record because they evidence the basis of admission and may be relevant to later revalidation.
- For unsuccessful applications, the application/CV, supporting evidence, vetting information, referee information, assessment/scoring record and decision/outcome are normally retained for 3 months after the final decision to allow for any challenge or appeal. Where no challenge is made, these records are securely deleted at the end of that period. Where a challenge or appeal is made, relevant information is retained until the matter is concluded and for any further period required for complaints, legal claims or other applicable requirements. We may retain anonymised statistical information for reporting and service improvement.
- CPD/professional-development records are retained during active membership and normally for the same post-membership period where they are needed to evidence progression or revalidation.
- Event registration and dietary/accessibility information is normally retained for 12 months after the event; finance records are normally retained for 7 years; and general enquiries are normally retained for 6 months after closure unless they become part of another formal record.
- Routine event photography is reviewed and normally retained for up to 3 years where it continues to have publication or promotional value; selected institutional archive material may be kept longer.
- Complaints, conduct and disciplinary information is retained according to the nature and outcome of the matter and any relevant legal or professional-standards requirements.

14. How we protect personal information

We use appropriate technical and organisational measures designed to protect personal information against accidental or unlawful loss, alteration, disclosure, access or misuse. These include, as appropriate, authenticated accounts, multi-factor authentication, role-based access, encryption and platform security controls, logging and monitoring, backups, incident management, staff training, confidentiality obligations, supplier due diligence and testing of significant system changes before release.

15. Keeping information accurate and re-establishing contact

We take reasonable steps to keep personal information accurate and up to date. Members can review and amend much of their information through the Members' Portal. Please tell us if important information changes or if you identify an error.

If we are unable to contact a current or former member using the information they supplied, we may make a limited and proportionate attempt to re-establish contact using publicly available professional information, such as LinkedIn or a previous employer. We do not use public sources to routinely enrich member profiles or for unrelated profiling.

16. Cookies and similar technologies

We use cookies and similar technologies to provide our websites and online services and, where you consent, to understand how our services are used. Our cookie-consent mechanism prevents non-essential cookies and tracking technologies from operating until the appropriate consent has been obtained and allows you to accept, reject or manage your preferences. You can change or withdraw those preferences at any time.

Our Cookie Notice explains the categories of cookies and similar technologies we use, their purposes and duration, third-party providers, relevant international processing and how to manage your preferences.

17. Your data protection rights

Depending on the circumstances, you may have the right to:

- be informed about how we use your personal information;
- request access to personal information we hold about you;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information in certain circumstances;
- ask us to restrict processing in certain circumstances;
- object to processing based on legitimate interests and object at any time to direct marketing;
- receive information you provided to us in a portable format where the right applies;
- withdraw consent at any time where processing is based on consent; and
- challenge certain solely automated decisions where applicable.

Your right to object: Where we rely on legitimate interests, you have the right to object to that processing. You also have an absolute right to object at any time to the use of your personal information for direct marketing.

These rights are not absolute and exemptions may apply. We may ask for information necessary to verify your identity before responding. We will normally respond within one month, subject to any lawful extension.

18. Complaints

If you have a concern about how we use your personal information, please contact our Data Protection Lead, Vikki Fox, at Vikki@security-institute.org. We will investigate and respond appropriately.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection. Current information on making a data protection complaint is available at ico.org.uk/for-the-public/how-to-make-a-data-protection-complaint/

19. Links, third-party services and social media

Our websites, applications and communications may contain links to services operated by other organisations. Those organisations are responsible for their own privacy practices. Your interaction with social-media platforms is also governed by the platform provider's terms and privacy information.

20. Changes to this notice

We may update this notice when our activities, systems, suppliers or legal obligations change. The latest version will be published on our website. Where a change is material, we will take reasonable steps to bring it to the attention of affected individuals.

21. Version history

Version	Date	Summary	Approved by
2.0	10 September 2026	Updated standalone Privacy Notice, including current retention, AI, cookie, PECR and data-protection transparency arrangements.	Chief Executive Officer