Elstree and District Scouts
C/O The Scout Association,
Gilwell Park,
Chingford, London,
E4 7QW
Registered Charity No. 1189643

Scouts
Elstree and District

POLICY NAME	Data Protection, Privacy and Data Retention			POLICY NO.	
EFFECTIVE DATE	25/02/2026	DATE OF LAST REVISION		VERSION NO.	2.0

VERSION HISTORY				
VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR

Table of Contents

1. Purpose, Status and Definitions

1.1 This Privacy and Data Protection Policy ("Policy") sets out how Elstree and District Scouts ("the District", "we", "us", "our") collects, uses, stores, shares and protects personal data, and how individuals may exercise their rights under data protection law.
1.2 This Policy is a formal governance document adopted by the District Trustee Board. It applies to all personal data processed by the District in connection with: (a) District Sections; (b) District-organised activities, events and training; (c) District governance, administration and communications; and (d) District-provided services and infrastructure used by Scout Groups within the District.
1.3 This Policy is intended to ensure compliance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, and applicable privacy laws including the Privacy and Electronic Communications Regulations (PECR) where relevant (e.g., cookies and electronic marketing).
1.4 This Policy must be read alongside: (a) Appendix A (Data Retention Schedule); (b) Appendix B (Cookies and Tracking); (c) Appendix C (Record of Processing Activities); (d) Scouts safeguarding policy and procedures, including the Yellow Card; and (e) any local procedures adopted by the District Trustee Board.
1.5 Definitions: "personal data", "special category data", "processing", "controller", "processor", and "data subject" have the meanings given in the UK GDPR. "Young person" refers to members under 18. "Parent/guardian" refers to a person with parental responsibility or legal guardianship.

2. Data Controller, Contacts and Accountability

2.1 Elstree and District Scouts is a registered charity with the Charity Commission for England & Wales.
2.2 The Data Controller for personal data processed by the District is the Elstree and District Scouts Trustee Board, acting collectively as Charity Trustees.
2.3 The Trustee Board appoints the District Lead Volunteer and the District Chair as joint Data Leads to oversee data protection compliance, provide assurance to trustees, and coordinate responses to data protection enquiries and incidents.
2.4 All data protection enquiries, subject rights requests and complaints must be directed to: support@elstreescouts.org.uk. Enquiries will be triaged and escalated to the appropriate Trustee, Data Lead, relevant team lead, or safeguarding lead.
2.5 The District maintains internal accountability records including: (a) this Policy; (b) the Retention Schedule; (c) the ROPA; and (d) where needed, Data Protection Impact Assessments (DPIAs) for higher-risk processing (for example, new systems collecting children's data at scale, or new tracking technologies).

3. Scope and Data Subjects

3.1 This Policy applies to personal data relating to:
3.1.1 Adult volunteers, trustees and other adults engaged in District roles;
3.1.2 Young people who are members of District Sections;
3.1.3 Adults and young people participating in District activities, events and training (including non-members);
3.1.4 Parents/guardians and emergency contacts;

3.1.5 Individuals submitting ‘want to join’ or membership enquiries, including those on District-wide waiting lists;
3.1.6 Donors, funders and Gift Aid declarants; and
3.1.7 Members of the public, suppliers and partners who contact the District.

4. What Data We Process and Where It Comes From

4.1 We process personal data obtained from multiple sources, including: individuals directly; parents/guardians; the Scouts HQ membership system and associated processes; event booking systems; online forms; email; and limited paper records where digital capture is impractical.
4.2 The District processes personal data across the following main processing streams:
4.2.1 Adult volunteer administration (including data held in the Scouts HQ membership system and mirrored into local District systems).
4.2.2 District activities, events and training (including bookings, registers, welfare and emergency planning).
4.2.3 District Sections (programme delivery, attendance, badge and award tracking, and welfare notes where necessary).
4.2.4 ‘Want to join’ enquiries and District-wide waiting lists (to allocate places across Groups).
4.2.5 Fundraising and Gift Aid (including donor records and HMRC submissions).
4.2.6 Governance and compliance (minutes, trustee records, policies, incident and insurance correspondence).
4.3 Categories of personal data we may process include:
4.3.1 Identity and contact data: name, address, email, phone number, date of birth, membership number, role details.
4.3.2 Participation data: attendance, event sign-ups, programme/badge records, training records and outcomes.
4.3.3 Welfare and safety data (special category): medical conditions, dietary requirements, accessibility needs, emergency contacts.
4.3.4 Safeguarding and incident data: incident reports, statements, communications, and outcomes (handled with strict controls).
4.3.5 Financial data: donations, Gift Aid declarations, payments for events/training, and related audit records.
4.3.6 Communications and technical data: emails, website analytics, cookie identifiers, device/browser data (where enabled by user choice).

5. Children’s Data and Additional Safeguards

5.1 The District recognises that processing children’s personal data requires additional care and safeguards.
5.2 Data for young people under 18 is ordinarily provided by parents/guardians; however participation data is generated through attendance, programme delivery and administration. District Sections may also maintain internal welfare/behaviour notes where necessary to operate safely and support the young person appropriately.
5.3 For Explorers (typically aged 14–17), we acknowledge that young people may sometimes provide information directly in addition to parental oversight.

5.4 The District uses appropriate access controls and limits data sharing for young people, including progressive disclosure of waiting list details to Groups as an enquiry progresses (see section 7).
5.5 Data subject rights for individuals under 18 are normally exercised by parents/guardians, except where legally appropriate.

6. Purposes of Processing and Lawful Bases

6.1 We process personal data for the following purposes: administering membership and volunteering; delivering safe activities and events; communicating operational information; managing waiting lists; governance and compliance; safeguarding and welfare; fundraising and Gift Aid; and promoting Scouting (including photography/video).
6.2 Lawful bases (UK GDPR Article 6) used by the District include:
6.2.1 Performance of a contract or arrangement (Art. 6(1)(b)) – e.g. administering participation in events or volunteering arrangements.
6.2.2 Legitimate interests (Art. 6(1)(f)) – e.g. District operational communications, waiting list management, governance, and promotion of Scouting, balanced against individuals' rights.
6.2.3 Legal obligation (Art. 6(1)(c)) – e.g. charity governance requirements, HMRC compliance (Gift Aid), insurance and statutory reporting.
6.2.4 Vital interests (Art. 6(1)(d)) – e.g. emergency medical situations.
6.3 Special category data (UK GDPR Article 9) is processed primarily under:
6.3.1 Legitimate activities of a not-for-profit body (Art. 9(2)(d)) with appropriate safeguards (e.g. medical/dietary information for events).
6.3.2 Substantial public interest / safeguarding grounds where applicable under UK law (e.g. where necessary to protect children).
6.3.3 Vital interests (Art. 9(2)(c)) in emergencies where consent cannot be obtained.
6.4 Safeguarding and welfare: Where safeguarding obligations apply, these may override or limit certain data subject rights where necessary to protect young people or comply with Scouts safeguarding procedures and legal duties.

7. 'Want to Join' Enquiries and District-Wide Waiting Lists

7.1 The District operates District-wide 'want to join' processes and waiting lists to manage demand for places across Groups and sections.
7.2 We process enquiry data such as: young person's name, age, postcode, section preference; and parent/guardian contact details.
7.3 Retention: 'want to join' data is retained until the young person reaches the age of 18, unless they join earlier or request removal.
7.4 Data sharing and visibility controls: to expedite placement while minimising unnecessary disclosure, data visibility increases as the process progresses:
7.4.1 Groups may view limited details (e.g., name, age, postcode and similar basic data) to determine whether to make an offer.
7.4.2 Groups may view full parent/guardian contact details once they have made an offer.
7.4.3 Groups may view full provided details once an offer is accepted by the parent/guardian.
7.5 Communications: the District may periodically contact enquirers to confirm they remain interested in a place. These contacts are operational and not marketing.

7.6 Removal requests should be sent to support@elstreescouts.org.uk; where lawful and appropriate, data will be removed from local systems and Groups notified.

8. Communications, Email Management and Messaging

8.1 The District uses email and messaging to deliver Scouting operations, including responding to enquiries, coordinating events, and communicating governance updates.
8.2 Authoritative record: the District designates District-managed mailboxes (including support@elstreescouts.org.uk) as the authoritative record for inbound enquiries and operational correspondence.
8.3 Use of personal email: Volunteers are expected to use District-provided email accounts wherever reasonably practicable. Where personal email accounts are used, relevant correspondence should be forwarded to a District-managed mailbox to support continuity and accountability.
8.4 Forwarding to personal inboxes: Volunteers are strongly discouraged from forwarding District correspondence to personal inboxes. Where this occurs, the District cannot control retention within personal email services and does not treat personal inboxes as systems of record. Volunteers are asked to delete Scouting correspondence from personal inboxes when no longer required.
8.5 One-size retention rule for District mailboxes: To ensure consistent retention without reliance on volunteer classification, automated retention rules apply to District-managed mailboxes. Routine correspondence is retained for up to seven (7) years and then securely deleted.
8.6 Safeguarding by email: Email is treated as a communication channel and not the definitive record of safeguarding concerns. Safeguarding information received by email is escalated promptly in line with Scouts safeguarding procedures and recorded/managed in the appropriate system and manner.
8.7 WhatsApp communities: the District may invite volunteers and, where appropriate, parents/guardians to join WhatsApp communities or groups for timely operational communication. Participation is voluntary and subject to WhatsApp's terms and privacy practices. Sensitive personal data should not be shared in WhatsApp groups.
8.8 Opt-out: Individuals may opt out of non-essential communications by emailing support@elstreescouts.org.uk (note that some operational communications may still be necessary for safety and administration).

9. Photography and Video

9.1 Photography and video recording may take place at District activities, events and training.
9.2 Individual image-by-image consent is not collected. Photography/video is addressed through event terms and participation conditions because of the scale and practical limitations of managing consent across large events.
9.3 Lawful basis: We rely on legitimate interests for photography/video used to promote Scouting, report on activities, celebrate participation and achievements, and maintain historical records.
9.4 Uses: Images/video may be used across websites, social media, printed materials, fundraising and grant applications, press/media, presentations, and other communications.
9.5 Retention: Images/video may be retained as part of the District's historical archive for up to 100 years.

9.6 Third-party photographers: the District may engage third-party photographers or media providers. Where engaged, they are expected to comply with data protection law and their own privacy obligations, and the District will apply appropriate contractual and governance safeguards where reasonably practicable.
9.7 Removal requests: Individuals may request removal of a specific identifiable image by contacting support@elstreescouts.org.uk. The District cannot guarantee it can identify all images of an individual across all historic resources but will make reasonable efforts to remove the specified image from future resources and prevent future use where practicable.

10. Systems, Processors, Access Controls and Security

10.1 The District uses digital systems to administer Scouting and deliver services, including: Microsoft 365 (email, storage, Teams), TicketTailor (event and training bookings), Cognito Forms (data collection), and website analytics/embedded services (e.g. Google Analytics, Microsoft Clarity).
10.2 We do not list every minor tool or plug-in in this Policy; however, we aim to be transparent about key processors and categories of tools used. Other systems and services may be used from time to time where appropriate; where this occurs, the District will seek to ensure suitable data protection safeguards are in place.
10.3 Access controls: Access to personal data is role-based, restricted to those with a legitimate need to know, and reviewed periodically. Waiting list data is accessible to the District team and relevant nominees from each Group. Safeguarding-related data is restricted to those strictly necessary, usually Scouts HQ and the District Lead Volunteer (or an authorised representative). Gift Aid records are accessible to relevant section/team leads, District leadership, and the Trustee Board.
10.4 Microsoft 365 security: District accounts are issued as individual named accounts (no shared logins) and multi-factor authentication is enabled.
10.5 Personal devices: Volunteers may access District systems using personal devices. While the District cannot impose technical standards for personal devices, it will take reasonable steps to reduce risk where devices are lost or compromised (for example, revoking access, resetting credentials, or disabling accounts). Volunteers are encouraged to report lost devices or suspected compromise promptly.
10.6 Data minimisation: The District seeks to collect and share the minimum personal data needed to deliver safe Scouting and meet legal obligations.
10.7 International transfers: Some services used by the District may process data outside the UK. Where relevant, the District relies on appropriate safeguards provided by those services (such as adequacy decisions or standard contractual clauses).

11. Sharing Personal Data

11.1 The District may share personal data where necessary and proportionate with:
11.1.1 The Scout Association and its national systems (including membership administration and safeguarding processes);
11.1.2 Scout Groups within the District (including waiting list management and membership offers);
11.1.3 Awarding bodies for externally accredited training (as independent controllers);
11.1.4 Insurers and professional advisers where needed (e.g., Unity Insurance Services); and

11.1.5 Statutory agencies, local authorities or law enforcement where required for safeguarding or legal reasons.
11.2 The District does not sell personal data.
11.3 Where third-party processors are used, the District seeks to ensure appropriate contractual and security safeguards are in place where reasonably practicable for a volunteer-led charity.

12. Data Retention, Records Management and Archiving

12.1 The District retains personal data only for as long as necessary for the purpose for which it was collected, and in accordance with Appendix A (Data Retention Schedule).
12.2 Emails: District-managed mailboxes apply a standard retention of up to seven (7) years then secure deletion, unless the content has been captured in another record that requires longer retention (e.g., governance minutes archived, or Gift Aid records).
12.3 Meeting minutes and governance records: Trustee Board minutes and formal governance records are retained for a minimum of six (6) years to meet legal, regulatory and audit requirements, and may be retained for up to one hundred (100) years as part of the District's historical archive.
12.4 Safeguarding records: The retention of safeguarding records is managed in line with Scouts safeguarding policy and procedures; the District does not rely on local email systems as the record of safeguarding concerns.
12.5 Secure disposal: The District will dispose of personal data securely when no longer required (for example, secure deletion of electronic files and confidential disposal of paper records).

13. Data Subject Rights and How to Exercise Them

13.1 Individuals have rights under data protection law, including the right to be informed, access, rectification, erasure (in certain circumstances), restriction, objection, and data portability (where applicable).
13.2 Requests should be submitted to support@elstreescouts.org.uk. We may request information to verify identity before responding.
13.3 We will respond within statutory timeframes. Where a request is complex or numerous, the District may extend the response time as permitted by law, and will inform the requester.
13.4 The District may refuse or limit a request where a lawful exemption applies, including where safeguarding or legal obligations require retention or disclosure.
13.5 Complaints: Individuals may raise concerns with the UK Information Commissioner's Office (ICO) via the ICO website.

14. Personal Data Breaches

14.1 A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
14.2 Suspected breaches must be reported promptly to support@elstreescouts.org.uk so the District can assess risk, contain the incident, and take corrective action.
14.3 Where required, the District will notify the ICO and/or affected individuals within the timescales set by law.

15. Cookies and Website Tracking

15.1 District websites may use cookies and similar technologies. A cookie banner is used to provide information and capture/record user preferences for non-essential cookies where required.
15.2 The District uses (subject to cookie choices) services such as Google Analytics and Microsoft Clarity, and may embed third-party services such as Cognito Forms and TicketTailor widgets.
15.3 Appendix B provides further details on categories of cookies and the purposes they serve.

16. Review and Document Control

16.1 This Policy is reviewed at least annually by the District Trustee Board and may be updated sooner if legal requirements, Scouts policy, or District systems/processes change.
16.2 This Policy supersedes prior local privacy notices adopted by the District Trustee Board.

Appendix A – Data Retention Schedule

A.1 This schedule forms an integral part of the Policy. Retention periods are based on Scouts retention guidance and local operational requirements. Where safeguarding concerns are involved, retention is handled in line with Scouts safeguarding procedures.

A1. Young People

Data Process	Data Type	Retention	Justification
Pre-join / waiting list enquiries	Personal data	Until age 18 or until earlier withdrawal	Required to manage District-wide waiting lists and placement offers
Joining / membership records	Personal + special category data	10 years after young person leaves	Required for membership enquiries and responding to statutory agencies regarding incidents
Events	Personal + special category data	2 years after event	Required for enquiries on the event and responding to incidents
Safeguarding	N/A – see Scouts safeguarding policy	N/A – see Scouts safeguarding policy	Safeguarding records managed under Scouts safeguarding procedures
Incident – no medical intervention	Personal + special category data	7 years after incident, or 7 years after individual turns 18 (if later)	Potential legal claims
Training records	Personal data	2 years after young person leaves	Required for any re-joins to connect them back to training records
Attendance register	Personal data	18 months	Required to complete annual registration review; supports Gift Aid where applicable

HQ youth award registrations	Personal + special category data	6 months after award completion	Retain registrations for the duration of eligibility period
HQ youth award completions	Personal + special category data	6 months after award completion (core award record retained nationally)	Historic record of award completions
Photos/videos (District archive)	Images/video	Up to 100 years	Historical archive; promotion and reporting

A2. Adult Volunteers

Data Process	Data Type	Retention	Justification
Pre-join enquiries	Personal data	1 year after enquiry or until adult joins	Required for recruitment and follow-up
Joining / membership records	Personal + special category data	2 years after adult volunteer leaves	Required for enquiries on membership
Adult Information Form	Personal + special category data	12 months or until checks and “Getting Started” training complete (whichever shorter)	Required to assist in appointment process
Identity checking record	Personal data	Until vetting process is complete	Required to verify identity has been checked
Events	Personal + special category data	2 years after event	Required for enquiries on event and incidents
Safeguarding	N/A – see Scouts safeguarding policy	N/A – see Scouts safeguarding policy	Safeguarding handled under Scouts procedures
Incident – no medical intervention	Personal + special category data	7 years after incident, or 7 years after individual turns 18 (if later)	Potential legal claims
Training records	Personal data	2 years after adult volunteer leaves	Required for any re-joins to connect them back to their training records
Appointments advisory notes	Personal data	18 months	Required to review training needs of adult volunteers

Adult award registrations	Personal + special category data	6 months after award completion	Retain registrations for eligibility duration
Adult award completions	Personal + special category data	6 months after award completion (core record retained nationally)	Historic record

A3. Parents and Guardians

Data Process	Data Type	Retention	Justification
Pre-join enquiries	Personal data	Until child reaches 18 or joins earlier	Required for placing individual on waiting list
Joining (contact details)	Personal data	2 years after young person leaves	Required for enquiries on membership
One-off events	Personal data	2 years after event	Required for event enquiries/incidents
Incident – no medical intervention	Personal data	7 years after incident, or 7 years after child turns 18 (if later)	Potential legal claims

A4. Donors and Gift Aid

Data Process	Data Type	Retention	Justification
Individual givers	Personal data	1 year	To keep you informed of your donation
Gift Aid declaration	Personal data	6 years after donation	HMRC tax audit
Gift Aid claim records	Personal/financial data	6 years	HMRC compliance
Direct debit mandate (if used)	Personal/financial data	6 years after last direct debit	Proof of instruction and assist in claims

A5. Governance and Corporate Records

Data Process	Data Type	Retention	Justification
Trustee Board minutes and governance records	Corporate records (may include personal data)	Minimum 6 years; archive up to 100 years	Legal/regulatory audit plus historical archive
Subject Rights Request (SRR) log	Personal data	7 years	Allow answers to queries/complaints relating to SRR

Insurance correspondence and claims	Personal data	6 years after closure (or longer if required)	Insurance/audit/legal claims

A6. Staff

Elstree and District Scouts does not employ staff at the time of this Policy version. If staff employment begins, this schedule must be updated accordingly.

Appendix B – Cookies and Tracking

B.1 This appendix summarises cookie and tracking categories used on District websites. Actual cookies may vary depending on site configuration and user preferences. Users manage preferences via the cookie banner.

Category	Examples	Purpose	Typical data captured
Essential/strictly necessary	Session cookies; security cookies	Enable core site functions, security, and preference storage	Session identifier; security tokens
Analytics	Google Analytics	Measure site usage and improve content	Pages visited; approximate location; device/browser info
Behavioural/UX analytics	Microsoft Clarity	Understand how users interact with pages to improve usability	Interaction events; device/browser info
Embedded services	Cognito Forms; TicketTailor widgets	Enable embedded forms and booking functionality	Form/session identifiers; interaction data

Appendix C – Record of Processing Activities (ROPA)

C.1 The District maintains an internal Record of Processing Activities in accordance with UK GDPR Article 30. The table below provides a populated starting point and should be updated when systems or processes change.

Processing activity	Purpose	Data subjects	Categories of data	Lawful basis	Recipients	Retention	Security measures
District volunteer administration	Manage appointments, compliance, training and governance	Adult volunteers, trustees	Contact details; role; training; permits; compliance; disclosure status metadata	Art.6(1)(b); Art.6(1)(f)	Scouts HQ; District leadership	Per Appendix A (A2)	M365 named accounts; MFA; role-based access
District communications (email)	Operational communication and governance updates	Adult volunteers; parents/guardians (where relevant)	Email address; name; role/relationship; correspondence content	Art.6(1)(f)	District team	7 years (mail box retention rule)	M365 retention policy; MFA; access reviews
Want to join waiting list	Manage demand and allocate places	Young people; parents/guardians	Name; age; postcode; parent contact details	Art.6(1)(f)	Groups within District (progressive visibility)	Until age 18	Restricted access; audit trails where available
District events and activities	Deliver safe activities and manage attendance	Young people; adults	Attendance; emergency contacts; medical/dietary (SC)	Art.6(1)(b); Art.9(2)(d)	Event leadership; insurers; Scouts HQ (if needed)	2 years after event (plus incident rules)	Access restrictions; secure storage
Safeguarding	Protect young people and	Young people; adults	Incident details; statement	Legal obligation;	Scouts HQ; statutory agencies	Not retained	Need-to-know;

escalation	comply with policy		s; contact info (may include SC)	safeguarding		locally (handled per Scouts policy)	secure transfer
Accredited training delivery	Administer accreditation/certification	Adults; young people	Attendance; assessment outcomes; certificates	Art.6(1)(b)	Awarding body (independent controller)	As required by awarding body	Secure transfer; restricted access
Gift Aid processing	Reclaim tax relief and comply with HMRC	Donors	Name; address; declarations; donation data	Art.6(1)(c)	HMRC	6 years	Restricted access; secure storage
Photography & media	Promote Scouting and maintain historical record	Young people; adults	Images/video	Art.6(1)(f)	Public (website/social/print)	Up to 100 years	Controlled publication; takedown on request where practicable