Deal, Walmer, Sandwich & District Scout Trustee Board

Data Protection Policy

Policy Issue No. : GDPR/001 **Vers 2.0**
Replaces : GDPR/001 Vers. 1.0

Prepared by: GDPR Sub-team

Authorised and Approved by: DWSD Scout Trustee Board

Chair or nominated representative: (sign) _____ (date) 15/01/2026

Implementation date 15th January 2026.

Distribution: All members of DWSDS Scout Trustee Board
(May be electronic).
DWSDS Website
Hardcopy master kept by GDPR Sub-team.
When revised, previous hard copy stored in District Archive.

This policy should be reviewed and formally approved each year at first District Trustee Board meeting following Annual General Meeting. The District Trustee Board, however, may agree to amend the policy at any time.

Date of Review	Policy Retained	Policy Revised	Chair or DTB representative Signature

CONTENTS

1.0 Overview

This document aims to provide easy to read guidance on GDPR compliance and promote awareness of how to keep information secure.

1.1 Who are we

Deal, Walmer, Sandwich and District Scout Council is an excepted charity* based in the South East UK area of Deal, Walmer, Sandwich, and surrounding villages.

Our mission is to actively engage and support young people in their personal development, empowering them to make a positive contribution to society. This has been our aim since 1910 and is only possible due to dedicated support from adult volunteers.

Our District Trustee Board (DTB) is the data controller for the information we collect from members' involvement in District activities. Any personal data that we collect is only in relation to the work we do with our members and through our relationship with supporters, donors and funders.

*An "excepted charity": This means the District is exempt from the requirement to register with the Charity Commission, but it still operates under charity law and has legal responsibilities, such as having charitable objects for public benefit, a governing body (trustees), and the need to keep proper accounts.

1.2 Personal data – what is it?

Personal data relates to a living individual who can be identified from that data. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

1.3 This Policy Affects

Who. Any individual with access to Scouting paperwork, systems or data.

What. Personal information of adult volunteers, young people, their families, including contact information, demographics, health conditions and behaviours.

1.4 Responsibilities

Learning. Completing Scout "Growing Roots" (Induction) and GDPR Familiarisation sessions are organisational requirements for all members.

Care. Our legal requirement is to be able to demonstrate that, at all stages, we have made reasonable efforts to keep private information safe from loss.

Accuracy. We are legally required to keep the data we hold accurate and store it for no longer than necessary (as defined in Data Retention, section 3.1).

Vigilance. If members find a system or process which they suspect is not compliant with this policy or in line with our security aims, they have a duty to inform the District Chair or District Lead Volunteer so it can be investigated.

Breaches. See Section 1.9

Leaving a role or the organisation. When a role ends, all relevant documentation relating to that role (in any format) including that which contains Personal Data is required to be passed to the District Lead Volunteer or the District Chair to pass on to the new role holder. Appendix 4, the GDPR Data Inventory must then be updated to include the new Data Holder.

1.5 Who is covered by this policy:

This policy applies to all adult members holding District roles or acting on behalf of the District. It also includes Group Lead Volunteers in their capacity as members of the District Team.

1.6 Purpose of policy:

This policy sets out Deal, Walmer, Sandwich and District Scout Council's approach to protecting personal data and explains members' rights and responsibilities in relation to how we process personal data.

It provides a structured and GDPR compliant approach to how data in its various forms is managed and safely disposed of by adults acting on behalf of the Scout District.

1.7 Procedures:

It is the duty of the role-holder associated with particular Process Areas and/or Data Processes including those listed in Appendix 4, "District Data Inventory" to act in compliance with this policy as a Data Processor on behalf of the DTB. Any concerns or practical difficulties encountered in carrying out these duties should be brought to the immediate attention of the DTB via the District Lead Volunteer and District Chair. Local arrangements may be made for the secure disposal of paper documentation, but this must always comply with section 3 of this policy.

1.8 Personnel Responsible for Implementing Policy

The DTB has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the District GDPR Sub-team. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the DTB who review this policy on an annual basis as a minimum, and after any major organisational change or event to ensure it meets current legal requirements and reflects best practice.
All District appointment holders have a responsibility for operating within the boundaries of this policy, and to report any finding of possible non-compliance. Questions regarding the content or application of this policy should be directed to the District GDPR Sub-team via the District Lead Volunteer or District Chair.

1.9 Breaches of Policy

Any person who knows or suspects that a breach of data security has occurred must report the breach immediately to the District Lead Volunteer and District Trustee Board Chair.

Appendix 1 The Data Breach Response Plan should then be followed by the District Trustee Board as a matter of urgency.

2 Data Security

2.1 Using Scouting-related Social Media

Care must be taken to respect personal data when using Scouting related-social media.

2.2 Using Scouting-related Internet

Care must be taken to respect personal data when using Scouting related internet sites. District may use internet searches to perform due diligence on candidates in the course of recruiting new adult volunteers or paid staff. Where we do this, District will act in accordance with its data protection and equal opportunities obligations.

2.3 Use of Email

Consider carefully who really needs to be copied on emails. Where appropriate, use CC: and BCC: facilities. For example, it might be appropriate to use CC: within a small group of people who already know each other. However, it would be more appropriate to use BCC: when emailing a large group of people who are not necessarily familiar with each other. When using BCC: provide a generic description of who the email has been shared with (e.g. all District Cub Section Volunteers).

Personal information should be sent in a password protected attachment. The password should be shared using a different channel (e.g. text message).

2.4 Storing Information

Printed information. Documents containing Personal data should be held securely, in a locked cabinet for example. This can be a more secure method than uploading them to online services because of the vastly reduced access.

At scouting venues. Personal information must not be left unattended at Scout venues, including headquarters, event registration desks, and at camp. Care should be taken when manually transporting files between sites and should never be left visible in vehicles. While complete data security is difficult, reasonable attempts such as lockable office filing cabinets and portable locked file boxes should be used to prevent potential breaches of information.

Computers and Portable Drives. These should utilise full disk encryption option found on most modern computers and computers must be password protected.
Electronic Documents. All documents that contain personal information, wherever they are stored (e.g. hard drives, USBs, cloud and email servers) should be password protected.

3. Data Retention

3.1 Data Retention Periods

The table on the following pages shows the retention period for each data process area along with Justification and Disposal Methods.

The Scout Association provides a solely digital system for the process of adult role appointment and management. Their own data protection policies and instructions must be followed when using this system. Where local documentation is used, the following guidance should be followed:

Process Area	Data Process	Digital/Paper	Data Type	Retention	Justification	Disposal Method
Appointing Adults	Pre-Join Enquiry	Paper and Digital	Personal	1 year or completion of Appointment	Allows for delay/pause in progression	Shred/Delete
Administration	District Administration, Correspondence etc. (not covered elsewhere)	Paper and Digital	Personal	Retain for 100 years	Potential Scouting use. Archived in the public interest*.	Shred/Delete *Exempt
Unique & Individual District Events	Documentation	Paper and Digital	Personal & Sensitive	Sensitive data 1 year after event.	Enquiries and incident response. Non-sensitive archived in the public interest.	Shred/Delete
Repetitive District Events	Organisational Documentation	Paper and Digital	Personal	3 years after last event	Future Organisation. Archived in the public interest.	Shred/Delete
District Finance	General Communications	Paper and Digital	Personal	I year or completion of business	In case follow-up required	Shred/Delete
District Finance	Invoices/Receipts	Paper and Digital	Transaction	7 years or duration of warranty, whichever greater	HMRC Tax audit or Charity Commission Enquiry	Shred/Delete
Young People	Pre-Join Enquiries referred to Group/Unit	Paper and Digital	Personal	1 month after referral	In case follow-up required	Shred/Delete
Young People	District Organised Events where there is no Scout Group Involvement	Paper and Digital	Personal and Sensitive	2 months after event	Required for enquiries concerning the event and responding to incidents	Shred/Delete
Young People – Explorer Scouts	District Explorer Scout Membership Records	Paper and Digital	Personal and Sensitive	1 year after Explorer leaves or Pass to Network on section change	In case of re-join or follow-up required	Shred/Delete
Young People – Network Scouts	District Network Scout Membership Records	Paper and Digital	Personal and Sensitive	1 year after Networker leaves	In case of re-join or follow-up required	Shred/Delete

HISTORICAL ARCHIVE						
District Archive	Storage on Local Database	Digital	Personal	Retain for archive	Potential Scouting matters contact for Reunions / History & Archiving in the public interest*.	*Exempt
District Archive	Advisory Committee Notes	Paper & Digital	Personal	Retain for archive	Archiving in the public interest*	*Exempt

4. Privacy

4.1 How the DTB gather personal information

The majority of personal information provided by adult members is held on the Scout Association Membership System. Any data, from time to time, held by District is, in most instances, obtained from this source, and held temporarily following their confidentiality requirements. In the case of young people, it is provided by parents or legal guardians. This may be in paper form or digital form and stored securely.

4.2 How do the DTB process our members' personal data?

The DTB comply with their obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure, and by ensuring that appropriate technical measures are in place to protect personal data.

The DTB process the data to be able to contact the member, parents and guardians; to inform them of meetings and events the district may be running or attending.

The DTB use personal data for the following purposes: -

- To collect personal and medical information for the protection of that person whilst in the care of the Scout District.
- To enable us to provide a voluntary service for the benefit of the public in our Scout District.
- To administer membership records
- To fundraise and promote the interests of Scouting across Deal, Walmer, Sandwich and District.
- To manage our volunteers
- To maintain our own accounts and records
- To inform volunteers of news, events, activities and services related to Scouting.

4.3 Sharing and transferring personal Information

The DTB share personal information within our Scout District with those who need to see it in the execution of their scouting roles.

On occasion the DTB share member's personal data with others outside our Scout District, such as when they need to meet or enforce a legal obligation. This may include The Scout Association, its insurance subsidiary "Unity", local authority

services, and law enforcement. The DTB only share members' personal information to the extent needed for those purposes.

The DTB never sell our members personal information to any third party for the purposes of marketing.

Member's personal data is treated as strictly confidential. Data is only shared with third parties outside of the organisation if there is a legitimate reason to do so. The DTB take steps to anonymise the data they provide (i.e. collective reporting on gender, ethnicity, age, etc.). If it is necessary to share identifiable data, the individual or guardian's consent will be sought.

4.4 Third Party Data Processors

Any third-party data processor that Deal, Walmer, Sandwich and District uses must also be GDPR compliant.

4.5 Transfers outside the UK

Deal, Walmer, Sandwich and District do not transfer members' personal information outside of the UK, except when an event is taking place outside of the UK and it is necessary to provide personal information to comply with legal obligations, although such an event is likely to have its own securely held data collection form that is disposed of after the event.

4.6 Member Rights and their Personal Data

Members have the right to access, correct, sometimes delete and restrict the personal information they use. In addition, they have a right to complain to the DTB and to the data protection regulator.

Unless subject to an exemption under the GDPR, members have the following rights with respect to their personal data: -

The right to be informed – members have a right to know how their data is used by the Scout District (as described in this policy).

The right to access personal data – members can ask the DTB to share the data that is held on them.

The right to rectification – members can notify the DTB and update (or have updated) their data if it's inaccurate or if something is missing. They can request to view, and have edited, any personal information that is held.

The right to erasure – members have the right to request that the DTB delete any personal data held about them when no longer a member. There are some exceptions, for example, some information can be held for legal reasons.

The right to restrict processing – If members think there's something wrong with the data being held about them, or feel the rules are not being complied with, the DTB can restrict any further use of their data until the problem is resolved.

The right to data portability – If a member asks, the DTB will share their data with them in a way that can be read digitally – such as a pdf.

The right to object – members can object to the ways their data is being used.

All enquiries should be referred in writing to the District Lead Volunteer or District Chair, in the first instance.

4.7 Subject Access Requests (SARs)

With these extensive rights available to data subjects it is important for the DTB to have a process in place for responding to a request from the data subject on any of the above. This is known as a subject access request (SAR). The response to the data subject must be within 1 month of receiving the request. This can be extended by a further month, followed by 1 more month if the request cannot be completed in time, but notice must be given to the data subject on the extension and the reason why.

The following contains guidance on processing such requests:
Any SAR made to the District must be referred to the District Lead Volunteer or District Chair.

Application - Data subject should be asked to complete a SAR Request Form (Appendix 2).

Identity Evidence - Data subject is required to provide photographic evidence of their identity. This can be in the form of a current passport or photocard driving license for example. (If a SAR is requested on behalf of someone else, both individuals must provide ID and a signed note appointing one to act on behalf of the other).

Request Logged - The date on which the identification checks and the specification of the data sought must be recorded in the SAR Register (Appendix 3).

Discovery - The DTB discovers all instances where the data subject's personal data is present. Appendix 4, "District Data Inventory" will help guide this.
Discovery entails either:
• Collecting the data specified by the data subject, or
• Searching all databases and all relevant filing systems (manual files) held by the Scout District including all available back up and archived files. (A separate SAR application is necessary for data held by The National Scout Association).

Response - DTB to respond to data subject in electronic format and response logged on Register.

The DTB is responsible for reviewing all provided documents to identify whether any third parties are identified in it and for either omitting or redacting identifying third party information from the documentation or obtaining written consent from the third party for their identity to be revealed.

If the requested data falls under one of the following exemptions, it does not have to be provided:

- Crime prevention and detection
- Negotiations with the requester
- Information used for research, historical or statistical purposes
- Information covered by legal professional privilege

In all cases care should be taken to redact all personal data or confidential information that the data subject should not see.

The information is to be provided to the data subject in electronic format unless otherwise requested, and all items provided should be recorded, in association with Appendix 3, in a document that shows the data subject's name and the date on which the information is delivered and stored securely.

4.8 Updates or changes to the Privacy Policy

The DTB reserve the right to make changes to this Privacy Policy.

5. Artificial Intelligence

5.1 Applicability of This Section

This section applies to all trustees, other volunteers, employees, contractors, and third-party representatives working on behalf of Deal, Walmer, Sandwich & District Scout Council. Its requirements should be reflected in other policies and procedures, agreements and contracts, as necessary.

5.2 AI Definition

Artificial Intelligence (AI) is defined as the ability of machines or software to perform tasks that would normally require human intelligence. AI systems can process data, learn from it, and make decisions or predictions based on that data. AI is a broad field that encompasses many different types of systems and approaches to machine intelligence, including rule-base AI, machine learning, neural networks, natural language processing and robotics.

5.3 AI Governance

All key AI decisions and proposals will be subject to scrutiny and approval by the Trustee Board. They will be advised on any concerns or breaches in AI use and will review this policy and our AI performance annually to keep up with evolving AI technologies and ethical standards.

Use of AI by our charity will have appropriate human oversight with humans being responsible for making all final decisions on their output. The board will maintain oversight by monitoring AI systems' performance, impact, and compliance with this policy on an ongoing basis.

To support this, the board will create any necessary guidelines on the collection, use and storage of data. This will ensure accountability for the decisions made by AI systems, which may include measures such as auditing, reporting and review processes and the use of algorithms in decision-making, including the steps to take to ensure these are as fair and unbiased as reasonably possible.

5.4 Management of Charity AI

The DTB will support our members in adapting to the changes AI will bring by providing them with appropriate support and skills development and taking into account their needs, when designing roles and work procedures.

The requirements of our AI policy will be embedded in other relevant policies and procedures, contracts, agreements and other documentation, such as job descriptions. The DTB will ensure that those in our charity with responsibilities for or involvement in AI, understand our charity AI policy, their responsibilities in delivering this and are accountable for doing so.

5.5 Charity AI Risk Management

The DTB's AI risk analysis has included any specific groups who may be at risk and other reasonably foreseeable uses of the technology, including accidental or malicious misuse. The risks have been identified and quantified, and the avoidance/mitigation action put in place will ensure that the level of risk remains within acceptable limits.

5.6 Charity AI - Data Protection & Privacy

As of January 2026 the DTB are in the process of updating their Data Protection Impact Assessment (DPIA) for AI and are making any necessary changes to their policies and procedures. As part of that, insofar as reasonably possible, the DTB will:

- Use accurate, fair, and representative data sets to ensure these are inclusive.
- Not include personal data in data sets, or at least pseudo-anonymise or de-identify it.
- Ensure the District's data consent procedures are always simple and clear and obtain user consent when using AI systems that process personal data.
- Reflect our use of AI in the District's privacy statement to ensure users know when their data is being used by AI, whether AI is making decisions about them and, if so, what these decisions are.

5.7 Charity AI Ethics

The DTB are committed to genuinely engaging with our stakeholders to ensure that our AI is aligned with their needs and values. The DTB factor into risk analysis any exclusion or detriment to stakeholders based on their identity. The board will take reasonable steps to avoid or minimise any exclusion or detriment and transparently communicate this. The DTB will ensure that any AI created content created respects the dignity of individuals and represents them in the way they would wish to be, including them being accurately depicted. For example, disability equipment or religious dress.

The DTB will make our AI systems and content as accessible as possible. Insofar as reasonably possible, they will use accurate, fair, and representative data sets to ensure these are inclusive. The board will ensure that any AI decisions are understandable and interpretable by stakeholders. This could involve documenting the logic behind AI decisions, providing clear explanations, and making sure that the reasoning is accessible to non-technical users.

All reasonable efforts will be made to identify any bias within an AI system the DTB use, to ensure any bias has either been eradicated or mitigated to the point where it is

within an acceptable level of risk. The DTB are open and transparent about any bias within an AI system (that they are aware of) and how they manage this.

Where AI is used to create content, there are appropriate checks and safeguards in place to ensure:

- Members are open and transparent that the content has been created by AI.
- AI created content is either self-evident or clearly identified and.
- It will not be used for purposes where the use of AI has been specifically not permitted.

There is appropriate content moderation by humans, to minimise the potential for errors and bias/defamatory phrases etc.

5.8 Environmental Considerations

The DTB are aware of the environmental impact of AI due to its very high energy consumption. The board will take this into account when considering our environmental impact and seek to make use of any emerging technologies that will help to minimise or mitigate this.

5.9 Charity AI Legal Compliance

The DTB will take all reasonable steps to identify copyrighted material. For any such material they use, they will ensure they have their copyright agreement, or it falls within 'fair use', or other exception to copyright, or the Open Government Licence (OGL), or some other free use category.

The DTB will not knowingly use any online material, such as from social media accounts or online galleries, which has been marked as 'NoAI', 'NoImageAI', or similar.

The DTB will take all reasonable steps to ensure that our use of AI does not have a negative impact on the legal rights and/or liberties of individuals or groups and complies with the Data Protection Act.

In particular, the DTB will ensure that for any AI use of their data, the data is clean, complete, compliant and they have appropriate consent, particularly the safeguarding of sensitive personal information.

5.10 Cyber Security

The DTB have robust cyber security procedures that everyone is aware of and complies with consistently to minimise the risk of AI scams.

5.11 AI Regulatory Guidance

- ICO - guidance on AI and data protection.
- ICO - AI and data protection risk toolkit.

6 Contact Details

If members want to contact us with any questions about this Data Protection Policy, or general matters relating to the way the board processes and hold data, please contact either the District Lead Volunteer or District Chair. Email: info@dealdistrictscouts.org.uk

7 Appendices

Appendix 1 – The Data Breach Response Plan

Appendix 2 – SAR Request Form

Appendix 3 – SAR Register

Appendix 4 – District Data Inventory