

	Gasóga na hÉireann / Scouting Ireland		
	No.	Issued	Amended
	SI-DP-04	24FEB2026	NA
	Next Review Date		
			FEB 2027
Category: Data Protection			
Scouting Ireland Data Retention policy			

Related Documents
SI-DP-01 Data Protection Policy

Revision Schedule		
Revision	Date	Description
1.0	24 FEB 2026	First Version of this document

Table of Contents

Table of Contents.....	2
1. Introduction	2
2. Scope.....	2
3. Legal and Regulatory Framework	3
4. Personal Data	3
5. Data Retention Principles.....	3
6. Data Categories and Retention Periods.....	3
7. Disposal of Data	7
8. Special Considerations for Sensitive Data.....	8
9. Storage and Security	8
10. Policy Review and Updates	8
11. Contact Details	8
12. Conclusion.....	9

1. Introduction

This policy sets out data retention times and disposal methods for records held by Scouting Ireland National office. A wide variety of records are held across Scouting Ireland National Office including but not limited to membership information, personal details of members, financial records, safeguarding and general administrative records. This retention periods described in this policy applies to records of all types regardless of the medium on which they are held. It is related to personal data held by National office only.

2. Scope

This policy applies equally to staff and volunteers within Scouting Ireland and covers both personal and sensitive personal data held in relation to its data subjects by Scouting Ireland. The policy applies equally to personal data held in manual and automated form. All personal and sensitive personal data will be treated with equal care by Scouting Ireland National Office. Both categories will be equally referred to as personal data in this policy, unless specifically stated otherwise.

Note: Scouting Ireland National office, together with the local Scout Groups, jointly manages the personal data of members stored in the Membership system (MMS), however National Office would be the primary controller for data retention within the MMS. While Scout Groups independently control the personal data they hold, Scouting Ireland National Office is responsible for managing all other personal data of members. See the Data Protection policy for more details.

This policy provides retention periods for personal data held at National level.

3. Legal and Regulatory Framework

Scouting Ireland is committed to ensuring compliance with the GDPR, particularly:

- **Article 5(1)(e)** of the GDPR, which mandates that personal data should not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.
- The **Data Protection Act 2018**, which supplements the GDPR in Ireland.

4. Personal Data

Personal data means any information about an identified or identifiable person. For example, an individual's name, home address, personal phone numbers and email addresses, occupation, photographs and so on can all be defined as personal data.

Some categories of personal data are recognised as being particularly sensitive ("special category data"). These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric information, data concerning health or data concerning a person's sex life or sexual orientation.

Personal data retention is governed by current Data Protection legislation. This data must be kept accurate, up to date, and retained for no longer than is necessary for the purpose for which it was obtained. Details of retention periods can be found in Table A – Retention periods.

Where an individual has requested the deletion of all personal data we hold about them, we may retain minimal personal data necessary to demonstrate that we have complied with their request.

5. Data Retention Principles

Scouting Ireland follows the following principles regarding data retention:

- **Data Minimisation:** Scouting Ireland will only collect data necessary for the intended purposes.
- **Retention period:** Personal data will be retained only for as long as it is necessary for the purpose it was collected. Once this period is over, data will be securely deleted or anonymised.
- **Review:** Retention periods will be regularly reviewed to ensure compliance with this policy.

6. Data Categories and Retention Periods

Scouting Ireland processes the following categories of personal data and retains them for the following periods:

Table A

Data Processing Activity	Retention Period	Reason for Retention
Membership Data held in the Membership system (MMS)	Active Membership – Data retained for duration of	Personal data of active members will be retained in

	membership	the membership system for as long as the individual remains an active member, to enable the organisation to manage participation, communication, safeguarding compliance, and insurance coverage.
	Inactive (up to 7 years) - Once a member leaves a Scout Group, they are updated to inactive status and end date added to their profile in the MMS with full data retained, restricted access is applied to the profile so only authorised members of staff have visibility to the profile.	To comply with statutory limitation periods and to allow time for potential legal claims, insurance matters, or safeguarding investigations to be raised. <i>Please note that if an investigation is ongoing when the retention period is reached, the data may be retained until the investigation has been formally concluded</i>
	Inactive 7 years from date of inactivation up to 100 Years Majority of personal data deleted: Only minimal identifiers retained (<i>Name, Membership number, Date of Birth, Group Name, Start and End date, training information and vetting dates if adult member</i>) with restricted access in place.	Minimal data is retained only for safeguarding and legal purposes. Retaining data for this length of time provides SI with the ability to support both former members and statutory authorities in any future investigations.
	Minimal personal Data is held in the MMS from 100 Years	Retained for historical purposes.
Safeguarding Case Management Records	Advice Files retained for 7 years from date of case closure. Safeguarding case management records are retained for 100 years from date of closure. However, related data and records may be deleted once the purpose has been fulfilled example notes related to the case. Periodic reviews will take place to ensure the retention period is still required and those identified as not required to be	This retention period reflects the need to preserve documentation that may be relevant to long-term safeguarding oversight or retrospective investigations.

	retained for the full retention period will be securely deleted.	
Disputes, Resolutions and Appeals Panel (DRAP) Records	DRAP case management files are retained for a period of 2 years following the closure of the appeals window. The appeals window closes 22 days after the DRAP case is officially closed	To comply with statutory limitation periods and to allow time for potential legal claims or investigations to be raised. <i>Please note that if an investigation is ongoing when the retention period is reached, the data may be retained until the investigation has been formally concluded.</i>
Accident / Incident Reporting (Insurance) records	Youth Member: Retained until the youth member turns 20 years old (plus 3 months).	Personal injury claims can be brought by minors up until they are 20 years old. <i>Noting if a case is opened and continues past the 20 years (plus 3 months) the data may be retained until the case is closed.</i>
	Adult Member: Retained for 7 years from the date of the Accident / Incident	To allow time for legal claims, insurance investigations, etc. <i>Noting if a case is opened and continues past the 7-year mark the data may be retained until the case is closed.</i>
Garda Vetting	Disclosures: Retained for three years from date of disclosure	Retained until the next Garda vetting occurs as used as a reference until the next vetting.
	Application: Hard copy of form(s) and copies of identification records retained for 6 months, after which it will be scanned and securely stored via National Office SharePoint and retained until the next vetting period (3 years) after which it will be securely deleted.	To comply with the Garda National Vetting Bureau process.
	Inactive volunteers: Once a volunteer leaves Scouting Ireland their Garda vetting related documentation will be	To comply with the Garda National Vetting Bureau process.

	deleted 12 months after their end date.	
Access NI	<p>Application Form: 6 Months from date of application</p> <p>Disclosure Certificate: 3 Years from date of disclosure</p>	<p>Application form retained to time for processing the application and allowing time for queries.</p> <p>Disclosure certificate: Used as reference until the next vetting renewal</p>
Email System (Scouts.ie emails)	Email correspondence: Scout.ie email accounts are retained for up to 7 years.	Governance and Legal purposes.
Expenses (ExpensIn system)	Financial Records containing personal data will be retained for 25 Years from the end of the financial report year for that record.	Preserve evidence for long-tail claims and regulated inquiries.
Iplicit	Financial Records containing personal data will be retained for 25 Years from the end of the financial report year for that record.	Preserve evidence for long-tail claims and regulated inquiries
National Camp Centre Bookings via Cinolla	Bookings are archived after 12 months and deleted after 7 years.	Campsite booking records are archived after 12 months for operational reference and deleted after 7 years to comply with statutory accounting, auditing, and insurance requirements, and to manage any potential legal claims arising from bookings.
Event Registration / Bookings via JotForm	<p>Information will be deleted from JotForm 3 months after the event.</p> <p>Confirmation of booking emails from JotForm to the Scouts Centre will be auto deleted after 7 years.</p>	Campsite booking records are retained for 7 years to comply with statutory accounting, auditing, and insurance requirements, and to manage any potential legal claims arising from bookings.
Photographs and Video Recordings at Scouting Ireland events	Photographs and video footage are collected by Scouting Ireland to showcase recent events on social media and other communication channels , and to promote future Scouting activities and events . Such images and videos are retained for up to five years from the date of	<p>To promote future events</p> <p>To preserve Scouting Irelands history</p>

	<p>capture or publication to support these promotional and communication purposes. After this period, materials are archived for historical and heritage purposes, recognising Scouting Ireland's legitimate interest in documenting and preserving its organisational history. Archived content is stored securely, with access restricted to authorised personnel, and is not reused for active promotional purposes unless renewed consent or a lawful basis is confirmed.</p>	
<p>Member wide email communications via Mailchimp</p>	<p>Email addresses are retained in Mailchimp for the duration of an individual's membership (applies to members 18 years and over only). The email list is refreshed every three months, or sooner if a new communication type is introduced, at which point a new upload of email data is performed. Communication types are reviewed regularly, and any outdated or irrelevant data is promptly removed from Mailchimp to ensure data accuracy and compliance with retention standards</p>	<p>Email data is retained to ensure that members receive timely and relevant communications regarding Scouting Ireland news, updates, and events. This supports effective engagement and ensures members remain informed throughout their membership</p>
<p>Subject Access Requests</p>	<p>2 Years from date of closure: All communications and personal data provided in response to the Subject Access Request will be deleted 2 years after the SAR is closed.</p>	<p>To demonstrate compliance with GDPR obligations and provide a record in case of follow-up queries.</p>
<p>Personal Data Breaches</p>	<p>7 Years from date of Breach: All communications and records of a personal data breach will be deleted 7 years after the date of the breach</p>	<p>To demonstrate compliance with GDPR obligations and provide a record in case of follow-up queries.</p>

7. Disposal of Data

Once the retention period for personal data has expired, the data will be securely deleted or

anonymised in a manner that protects the privacy of individuals. This may include:

- Securely and permanently deleting electronic data from all systems and devices.
- In some cases, depending on the personal data we might anonymise data in place of deleting it. This means the data is no longer identifiable and cannot be traced back to an individual. Where this happens this will be made clear to the data subjects.
- Shredding physical paper documents.
- In some cases we will apply automatic deletion processes, example with the scouts.ie accounts, emails older than 7 years will automatically be deleted.

8. Special Considerations for Sensitive Data

Some personal data may be classified as sensitive (e.g. health data). This data will be retained for the minimum necessary period, in accordance with legal and regulatory requirements. Special care will be taken in the secure storage and disposal of sensitive data. Regular reviews of sensitive data will take place throughout the lifecycle, and anything deemed no longer necessary will be securely deleted / destroyed. The Safeguarding department use Thread legal as their case management software; this has restricted access to the relevant Safeguarding team only.

9. Storage and Security

Scouting Ireland is committed to ensuring that personal data is always kept secure, whether held electronically or in physical form. Appropriate technical and organisational measures are in place to prevent unauthorised access, alteration, disclosure or destruction of personal data. Scouting Ireland uses Microsoft 365 to store and manage electronic records. All data within MS 365 is stored securely in accordance with Microsoft compliance and security standards, including encryption at rest and in transit, access controls, and regular security monitoring. Access is restricted to authorised personnel only.

10. Policy Review and Updates

This policy will be reviewed annually to ensure compliance with changes in legislation, regulations, and organisational needs. Any amendments to this policy will be communicated to relevant staff and stakeholders.

11. Contact Details

For any questions regarding this Data Retention Policy, or to exercise your data protection rights, please contact:

The Data Protection Officer dataprotection@scouts.ie

Or you can write to them at:

FAO: Data Protection Officer
Scouting Ireland
National Office
Larch hill

Dublin 16
D16 P023

12. Conclusion

By adhering to this Data Retention Policy, the Company ensures that it remains compliant with data protection laws, while also respecting the privacy and rights of its members, volunteers, staff, and stakeholders.