Scouting Ireland, National Office, Larch Hill, Dublin 16, Ireland.
T: 01 4956300
www.scouts.ie

	Gasóga na hÉireann / Scouting Ireland			
	No. SI-DP-03	**Issued** 22 Oct 2025	**Amended** NA	**Next Review Date** October 2027
	Category: Data Protection			
	Scouting Ireland Data Breach Policy			

Related Documents
SI-DP-01Data Protection Policy
SI-DP-02 Guidelines on managing personal data breaches
SI-DP-F02 Data Breach Report Template

Revision Schedule		
Revision	**Date**	**Description**
1.0	22 Oct 2025	First Version of this document

Scouting Ireland, National Office, Larch Hill, Dublin 16, Ireland.
T: 01 4956300
www.scouts.ie

Table of Contents

Scouting Ireland, National Office, Larch Hill, Dublin 16, Ireland.
T: 01 4956300
www.scouts.ie

1.0 Purpose:

This policy sets out how Scouting Ireland National Office and Scout Groups will identify, manage, report and document personal data breaches in accordance with the General Data Protection (GDPR) and Data Protection Act 2018.

2.0 Sope:

This policy and procedure applies to:

- All staff, volunteers, contractors, volunteer project teams, Board Members, Board Sub-committees, core teams, support teams and any other role that holds a Scouts.ie email address.
- **All personal data** processed by or on behalf of Scouting Ireland and/or Scout Groups, regardless of format (e.g. electronic, paper-based, verbal).
- **All locations, systems, and projects** where personal data is collected, stored, accessed, or otherwise handled.

3.0 Definitions

Data Protection Commission (DPC): The DPC is the national independent authority in Ireland responsible for upholding the fundamental right of individuals in the European Union (EU) to have their personal data protected.

Data Protection Officer (DPO): A DPO is a role established under the GDPR to ensure that an organisation processes personal data in compliance with the applicable data protection rules.

General Data Protection Regulation (GDPR): GDPR) is an EU law that regulates the collection, processing and storage of personal data, ensuring individuals privacy rights and imposing strict penalties for non–compliance on organisations handling such data.

Personal Data: As per GDPR Article 4 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: Defined in section 4

Special Categories of Data (Sensitive Data): Under GDPR Article 9 special categories of data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.0 Definition of a Personal Data Breach

As per GDPR Article 4(12) A personal data breach means a **breach of security** leading to:

- The accidental or unlawful destruction
- Loss
- Alteration
- Unauthorised disclosure of, or
- Access to, personal data transmitted, stored or otherwise processed.

Examples of a personal data breach include:

- An email with personal details about a youth member (e.g. medical condition or behavioural information) is sent to the wrong parent
- Disclosure of sensitive personal data without proper authority
- Paper records with personal or sensitive information are disposed of in a regular bin instead of being shredded
- Paper forms containing personal data, example medication record form or activity consent form left behind on public transport
- Sharing a youth members photograph on social media without appropriate consent
- A volunteer discussing a member's medical issue or behaviour concern in a public or inappropriate setting where others can hear.
- Cyberattack or system intrusions where personal data has been compromised
- Accessing personal data without a legitimate reason to do so
- Sharing your log in details to the membership database with another individual
- No access control in place for electronically documents containing personal data

5.0 Roles and Responsibilities

All Scouting Ireland staff, volunteers and members must report suspected breaches immediately.

For National level data breaches, the Data Protection Officer (DPO) (dataprotection@Scouts.ie) is responsible for:

- Investigating and assessing breaches with support / input from the relevant functional area
- Coordinating notifications to authorities and affected individuals
- Maintaining a data breach log
- Recommending remedial and preventive actions

For a Scout Group level data breach, the group leader or relevant data protection point of contact within the group is responsible for:

- Investigating and assessing breaches
- Coordinating notifications to authorities and affected individuals
- Notifying Scouting Irelands DPO (dataprotection@scouts.ie)
- Maintaining a data breach log
- Recommending remedial and preventive actions
- Please note that the relevant person in the Scout Group can always reach out to the DPO for support and guidance when it comes to a personal data breach.

6.0 Reporting a personal data breach

Any individual who becomes aware of a potential or actual personal data breach must:

1. Report it immediately to their DPO or Data Protection point of contact
    - Scouting Ireland Staff, contractors, Board members, Board Sub-committees, volunteer project teams, core teams, support teams and any other role that holds a Scouts.ie email address should notify the DPO (dataprotection@scouts.ie).
    - If a volunteer identifies a personal data breach tied to their Scout Group, then report it directly to the Scout Groups Data Protection Point of Contact or Group Leader.
    - If you are **unsure of who to go to, report it directly to the DPO** who can review and provide guidance as needed.

2. Include as much detail as possible about:
    - What happened

- When it happened
- Who and how many individuals were affected
- What data was involved
- What actions have been taken to contain the breach

There should be no delay in reporting, even if all the details are not yet available.

7.0 Assessment and Risk Evaluation

The DPO or data protection point of contact will assess:

- The nature and volume of the data involved
- The potential impact on individuals rights and freedoms
- Whether the breach meets the threshold for notifying:
    - The Data Protection Commission (DPC) and / or
    - The affected individuals
- A decision must be made within 72 hours of awareness of the breach. If 72 hours has passed, a personal data breach should still be notified, including a reason for the delay in notification.

8.0 Notification Process

If required:

- The Data Protection Commission (DPC) should be notified within 72 hours via the DPC Report a Breach function on their website www.dataprotection.ie)(GDPR Article 33 (1)).

- Individuals affected will be informed without undue delay if the breach presents a **high** risk to their rights and freedoms (GDPR Article 34 (1)).

- When personal data is collected, used, or shared, there is always a risk that someone's rights or privacy could be harmed. These risks can be minor or serious and may include things like emotional distress, financial loss, or harm to someone's reputation.

  Examples of risks include:

    - Discrimination, identity theft, fraud, or financial loss
    - Losing control over their own personal data
    - The use of sensitive information, such as a person's race, religion, health, political opinions, or sex life
    - Judging or profiling someone based on their data — like trying to predict their behaviour, health, or finances
    - Processing data about vulnerable people, especially children
    - Large amounts of personal data being handled in a way that affects many people

Notifications to an individual should include:

- Date the breach occurred
- A description of the breach i.e. what happened
- The types of data involved
- Immediate actions taken
- Risk assessment
- Next Steps
- Contact details for the DPO and Data protection point of contact if at group level
- Contact details for the Data Protection Commission if the affected individual wishes to make a complaint

9.0 Containment and Remediation

Scouting Ireland and / or the Scout Group will act quickly to:

- Stop or reduce the ongoing impact to the personal data breach
- Recover lost data where possible
- Secure systems or physical records

10.0 Record Keeping

As per GDPR Article 33(5) all breaches, regardless of whether they are notifiable, will be recorded in the Data Breach log maintained by the DPO. Each Scout Group will also maintain a log of data breaches which occur within their group. This log should contain at a minimum:

- The causes of the personal data breach
- What took place
- The personal data affected
- Effects and consequences of the personal data breach
- Remedial actions

All information relating to the personal data breach should be retained for six years from the date of the data breach.

11. Contact and Support

Any questions or support in relation to a personal data breach please contact the Data Protection Officer (dataprotection@Scouts.ie) or phone National office on 01 495 6300.