



Data Protection Policies

Designated responsible: <i>(Board Committee or Individual person)</i>	CEO in conjunction with Safeguarding Officer
Overall responsibility: <i>(Committee)</i>	Board
Effective from:	June 2026
To be reviewed:	June 2029

Change Log			
Version	List section numbers changed	Date	Author
2.0	Policies merged; structure/numbering updated; GDPR, retention & destruction sections revised; Appendix A added.	June 2026	Safeguarding & Data Protection Manager

Version numbering: Major Changes 1.0, 2.0; minor changes 1.1, 1.2

Change Tracking: All changes recorded and documented either via track changes or report outlining changes from previous version to the proposed version

Data Protection Policies

Contents

1. Purpose and Scope	3
2. Responsibilities	3
3. Policy Statement.....	3
4. Definitions.....	3
5. Procedures and Guidelines.....	4
5.1 Data Protection Principles.....	4
5.2 Data Subject Rights.....	5
5.3 Subject Access Requests (SARs)	5
5.4 Third-Party Processors.....	5
5.5 Data Breach Management.....	5
5.6 Data Retention.....	5
5.7 Data Destruction.....	6
5.8 Volunteer Data Protection Guidance.....	6
6. Compliance and Consequences	6
7. Appendix A: Data Destruction Procedures	7

1. Purpose and Scope

Irish Girl Guides (IGG) is committed to protecting the rights and privacy of individuals in accordance with EU General Data Protection Regulation (GDPR), the Data Protection Act 2018, and the EC Electronic Communications Regulations (2011).

This policy outlines IGG's obligations when handling personal data and provides a framework to ensure that Guiding activities are carried out safely, consistently, and lawfully.

This policy applies to all personal and sensitive personal data held by IGG in both manual and electronic formats. IGG processes personal data relating to employees, adult members, youth members and their parents/guardians, volunteers, third-party service providers, job applicants, customers, and suppliers.

This policy operates alongside IGG's Safeguarding Policy to ensure that youth data is handled in a manner consistent with child-protection obligations.

2. Responsibilities

IGG as Data Controller

IGG acquires, processes, and stores personal data as part of its daily operations. Staff and volunteers must consult the Data Protection Manager if unsure whether data may be disclosed.

Staff and Volunteer Responsibilities

All individuals who collect or process personal data on behalf of IGG must comply with this policy, follow confidentiality requirements, process data only for legitimate organisational purposes, and report concerns or breaches immediately. They must also ensure personal data is accurate and up to date, correcting or reporting inaccuracies promptly.

Third-Party Processors

Third-party processors must operate under written contract and comply with GDPR and IGG requirements.

3. Policy Statement

Irish Girl Guides is committed to ensuring that personal data is processed lawfully, fairly, and transparently, collected for specific and legitimate purposes, kept accurate and up to date, retained only for as long as necessary, and kept secure at all times.

All members, staff, and volunteers must follow this policy and related procedures.

4. Definitions

Personal Data

Personal data is any information about a living person that identifies them or could be used to identify them. This includes details such as name, date of birth, address, email, phone number, and financial information.

Special Category Data

Special category data is personal information that is more sensitive and requires extra protection. This includes data about racial or ethnic origin, religious or philosophical beliefs, health, or sexual orientation.

Data Subject

The individual to whom the personal data relates.

Data Controller

The organisation that determines how personal data is used — in this case, IGG.

Data Processor

A third party processing data on behalf of IGG.

Processing

Any operation performed on personal data, including collection, storage, retrieval, disclosure, and deletion.

Data Protection Manager (DPM)

The individual responsible for overseeing data protection compliance.

Data Breach

A security incident leading to accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data.

Retention Period

The length of time personal data is stored before being securely destroyed or anonymised.

5. Procedures and Guidelines

5.1 Data Protection Principles

IGG adheres to the seven GDPR principles:

1. Lawfulness, fairness and transparency – Personal data must be processed lawfully, fairly and in a transparent manner.
2. Purpose Limitation - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimisation – Personal Data must be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.
4. Accuracy – Personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted.
5. Retention – Personal data should be kept in an identifiable format for no longer than is necessary.
6. Integrity and confidentiality – Personal data should be kept secure.
7. Accountability – Organisations must not only comply with the above six general principles but must be able to demonstrate that they comply by documenting and keeping records of all decisions.

IGG processes personal data under the lawful bases of consent, contract, legal obligation, legitimate interests, and vital interests (for safeguarding or medical emergencies).

5.2 Data Subject Rights

Data subjects have rights including access, rectification, erasure, restriction, portability, and objection. For youth members under 18, parental or guardian consent is required for collecting and processing their personal data

5.3 Subject Access Requests (SARs)

All SARs must be referred to the DPM immediately. Responses will be issued within one month, with extensions up to three months for complex requests.

5.4 Third-Party Processors

IGG engages third-party processors such as Online Guide Manager. All processors must operate under written contract and comply with GDPR and IGG requirements.

Where data is transferred outside the EEA, IGG ensures appropriate safeguards such as Standard Contractual Clauses (SCCs) are in place.

5.5 Data Breach Management

A personal data breach includes accidental or unlawful destruction, loss, alteration, or unauthorised disclosure.

In the event of a breach:

- All staff and volunteers must report any suspected breach immediately to DPM, even where the risk is unclear.
- The DPM will investigate, document, and implement corrective actions.
- The Data Protection Commission must be notified within 72 hours except where the breach has been assessed as unlikely to present any risk to the rights and freedoms of data subjects.
- Data subjects must be informed when a breach is likely to pose a high risk, unless the data was protected (e.g., encrypted), the risk has since been removed, or contacting individuals would involve disproportionate effort.

5.6 Data Retention

IGG retains personal data only for as long as necessary to fulfil operational, legal, regulatory, or historical purposes.

Retention periods are defined in the IGG Data Retention Schedule. Data must be securely destroyed when no longer required.

5.7 Data Destruction

IGG securely destroys personal data in manual, electronic, and online formats.

High-level principles:

- Records must be destroyed promptly once retention periods expire.
- Secure methods must be used for both manual and electronic data.
- Third-party destruction providers must be vetted and contracted.
- Certificates of Destruction must be obtained.

Detailed procedures are set out in Appendix A.

5.8 Volunteer Data Protection Guidance

Irish Girl Guides provides separate *Data Protection Guidance Notes for Volunteers*. These notes summarise key volunteer responsibilities in a clear, practical format and must be read alongside this policy.

All volunteers must:

- follow the Volunteer Guidance Notes
- handle personal data in accordance with IGG policies and GDPR
- take reasonable steps to protect confidentiality
- seek advice where unsure

6. Compliance and Consequences

Failure to comply with this policy may result in:

- disciplinary action for staff/volunteers
- termination of contracts with third-party processors
- reporting to the Data Protection Commission
- legal liability, including fines or sanctions

Improper disposal of data may lead to:

- regulatory investigations
- penalties
- reputational damage
- loss of member trust
- costs associated with breach notification

All staff and volunteers must report suspected breaches immediately.

7. Appendix A: Data Destruction Procedures

(Supporting Document to Section 5.7 – Data Destruction)

A.1 Overview

Irish Girl Guides (IGG) recognises that personal data stored in manual (paper-based) or electronic formats cannot simply be discarded. Improper disposal poses risks including:

- unauthorised access
- data breaches
- reputational damage
- regulatory penalties

Paper files, hard drives, USB drives, CD-ROMs and other storage media may contain commercially sensitive or personal data. All such media must be securely destroyed using approved methods.

Electronic media must be securely wiped before destruction. Deleting or formatting a device is not sufficient, as data remains recoverable until overwritten. Secure erasure tools must be used in line with recognised standards such as NIST 800-88.

These procedures support IGG's obligations under Data Protection legislation to retain personal data only as long as necessary and to dispose of it appropriately. This appendix aligns with *IGG Data Protection Policies*.

A.2 Purpose

This appendix defines the operational requirements for the secure disposal of manual and electronic data within IGG.

A.3 Scope

These procedures apply to all personal data held by IGG in manual, electronic, or online formats.

A.4 Manual Data Disposal Procedures

A.4.1 Review and Scheduling

1. IGG will conduct regular reviews of manual records and schedule destruction when retention periods have expired, in line with the *IGG Data Retention Schedule*.
2. Records awaiting destruction must be stored securely.

A.4.2 On-Site Shredding for Short-Term Records

IGG maintains a locked confidential-waste bin on site for the disposal of short-term paper records. Staff place materials directly into the bin, which is collected and securely shredded by an approved third-party destruction provider.

3. Staff are advised to place short-term or low-risk materials into the confidential-waste bin for shredding, such as:
 - general office correspondence
 - handwritten notes
 - temporary reference copies

A.4.3 Third-Party Destruction for Bulk or Long-Term Records

4. A specialised third-party provider will be appointed to destroy medium- and long-term retention records.
5. The provider must sign a Data Processor contract.
6. Provider staff must be appropriately vetted in line with the company's own security requirements.
7. Destruction must occur on the same day unless unavoidable.

A.4.4 Required Steps for Secure Manual Data Destruction

8. The following steps must be followed:
 - a. Collate records at a designated secure IGG site.
 - b. Ensure the third party assumes full responsibility for collection and removal.
 - c. Ensure all materials are tagged prior to destruction.
 - d. Ensure adequate personnel are provided for efficient removal.
 - e. Require the third party to record an inventory of materials before destruction.
 - f. Place all records in secure bags or cartons before loading.
 - g. Appoint IGG staff to witness shredding and verify vehicle/site security.
 - h. Ensure shredding reduces materials to cross-cut debris no larger than 100mm² (e.g., 20mm × 5mm strips).
 - i. Obtain a valid Certificate of Destruction.
 - j. Require a documented action plan for incidents affecting the service.
 - k. Ensure environmentally responsible disposal of shredded materials.

A.5 Technology Equipment Disposal Procedures

A.5.1 Collection and Storage

1. IGG will schedule regular collection of end-of-life technology equipment.
2. Equipment must be stored securely prior to destruction.

A.5.2 Equipment Covered

This includes, but is not limited to:

- internal and external hard drives (HDD/SSD)
- RAM modules
- backup tapes (DAT/DLT/LTO)
- CD/DVD/Blu-ray media
- mobile phones and PDAs
- USB flash drives
- memory cards (SD/microSD)

A.5.3 Third-Party Destruction Requirements

3. A vetted third-party provider will carry out destruction using recognised industry standards, e.g., EN 15713:2009 for secure destruction of confidential material.
4. A Data Processor contract is required.
5. Provider staff must be appropriately vetted in line with the company's own security requirements.
6. Destruction must occur on the same day unless unavoidable.

A.5.4 Required Steps for Secure Technology Equipment Destruction

7. The following steps must be followed:
 - a. Collect equipment from a designated secure IGG site.
 - b. Ensure the third party assumes responsibility for packing and removal.
 - c. Tag all equipment prior to destruction.
 - d. Ensure adequate personnel for efficient removal.
 - e. Deliver, fill, and remove storage boxes/cages on the same day.
 - f. Complete an asset registry count before destruction.
 - g. Place equipment in sealed security boxes before transport.
 - h. Appoint IGG staff to witness destruction and verify security.
 - i. Ensure destruction reduces media to debris no larger than 20mm.
 - j. Obtain a valid Certificate of Destruction.
 - k. Require a documented action plan for incidents affecting the service.
 - l. Ensure environmentally responsible disposal of shredded materials.

A.6 Online Data Disposal Procedures

1. IGG will issue regular reminders to staff and volunteers to delete unnecessary online data.
2. This includes, but is not limited to:
 - OneDrive/Microsoft Teams
 - Microsoft Forms
 - SharePoint
 - Outlook Email Folders
 - Google Groups
 - Dropbox
 - Online Guide Manager
 - Any other online storage locations where IGG data may be held

A.7 Ramifications of Improper Disposal

Failure to properly dispose of personal data may result in:

- regulatory investigations
- fines and penalties
- reputational damage
- negative member perception
- costs associated with breach notification
- loss of trust in IGG

These risks reinforce the importance of following this appendix and the wider IGG Data Protection Policies.