The Federation of Astronomical Societies

UK GDPR Compliance Guide for Astronomical Societies

A Practical Handbook for Astronomy Groups

Version 3

April 2026

Document History

Date	Author(s)	Version	Comments
April 2026	Clare Lauwerys	3	Complete rewrite to make it more user friendly
03-Feb-2020	Paul Daniels	2.1	A small typo correction, one small clarification, removal of parentheses from '(GDPR)' in the header and repair of the automatic date fields in the title box and header.
05-Jan-2020	Graham Bryant	2.0	Updated as post GDPS Implementation
23-Apr-2018	Graham Bryant	1.0	Document released to membership
22-Apr-2018	Paul Daniels	0.2	Documents combined and re-formatted
20-Apr-2018	Graham Bryant/ Philip Johns	0.1	Document Created

Contents

1. Don't Panic! 3
2. Important Legal Disclaimer 3
3. Plain English Summary 3
4. How to Use This Guide 4
5. Purpose and Scope 4
6. Who This Guide Is For 4
7. Key Definitions 4
8. Data Lifecycle 5
9. Common Misunderstandings 5
10. Practical Examples of Good and Poor Practice 6
11. The Five Core Duties 6
12. Lawful Bases for Processing 7
13. Legitimate Interests Assessment (LIA) 8
14. Member Rights 9
15. Subject Access Request (SAR) Workflow and Template 9
16. Data Minimisation And Retention 10
17. Consolidated Retention Schedule 11
18. Data Security 11
19. Minimum Technical Standards 12
20. Data Breach Protocol 12
21. Data Breach Decision Tree 13
22. Special Considerations 13
23. Additional Considerations for Charitable Astronomical Societies 15
24. Guidance on Committee Minutes 16
25. Data Sharing with Partner Organisations 16
26. Data Processing Agreement Checklist 16
27. Annual Compliance Checklist 17
28. Annual GDPR Review Template 17

Appendix A — Privacy Notice Template 19
Appendix B — Data Audit Template 20
Appendix C — Record of Processing Activities (ROPA) 21
Appendix D — Data Breach Response Log 23

1. Don’t Panic!

This document may seem long but it contains useful appendices as well as the policy template.

2. Important Legal Disclaimer

This guide provides general information to help astronomical societies understand their responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Federation of Astronomical Societies is not a law firm, safeguarding authority, regulated professional body, or statutory agency. Safeguarding duties vary depending on an organisation’s legal structure, activities, jurisdiction, and risk profile. This template does not guarantee compliance with:

- Applicable legislation
- Statutory guidance
- Charity law
- Regulatory reporting obligations

Each adopting organisation is solely responsible for:

- Reviewing and adapting this template
- Obtaining independent professional advice where appropriate
- Ensuring compliance with relevant law

Use of this template is entirely at the adopting organisation’s own risk. To the fullest extent permitted by law, the issuing organisation disclaims all liability arising from reliance on this document.

Organisations are strongly advised to seek independent advice, particularly if they are registered charities.

3. Plain English Summary

This is guidance, not legal advice.

You must adapt it to your organisation.

If unsure, seek professional advice.

4. How to Use This Guide

This handbook is designed to be practical and easy to adopt. Committees can use it in several ways:

- New officers should read the Plain English Summary, the Five Core Duties, and the Annual Checklist.
- Data Protection Leads should use the templates in the Appendices to maintain documentation.
- Committees should review the Retention Schedule, Privacy Notice, and Data Audit annually.
- Societies adopting the guide should customise the Privacy Notice, Data Audit, and ROPA to reflect their own activities.
- When unsure, seek independent advice—especially if you are a registered charity or handle data relating to children.

This guide is not intended to be read in one sitting. It is a reference document to support day-to-day decision-making.

5. Purpose and Scope

Astronomical societies routinely collect and process personal data such as membership details, event registrations, Gift Aid information, volunteer records, and visitor logs. UK GDPR applies to all such activities. All organisations that handle personal data have to be compliant with these regulations.

This guide provides a clear, practical framework tailored to the needs of astronomy groups, helping committees meet their legal obligations in a proportionate and manageable way.

6. Who This Guide Is For

This guide is written for anyone involved in running, supporting, or overseeing an astronomical society, whether incorporated or unincorporated. It is particularly relevant to committee members, trustees, membership secretaries, treasurers, safeguarding and outreach leads, observatory managers, and volunteers who handle personal data as part of society activities. It supports both experienced officers and those new to committee roles by offering a practical, proportionate approach to GDPR compliance

7. Key Definitions

- **Personal Data** - Any information that can identify a living person (e.g., name, email address, phone number).
- **Processing** - Any action involving personal data, including collecting, storing, using, sharing, or deleting it.
- **Data Subject** - The individual whose data is being processed (e.g., a member or visitor).
- **Data Controller** - The organisation deciding how and why data is processed (the society).
- **Data Processor** - Anyone processing data on behalf of the controller (e.g., a cloud provider).

- **Joint Controllers** - Two or more organisations that jointly decide why and how personal data is processed. This may apply when running a shared event with a school, museum, or council etc. Joint controllers must agree their respective responsibilities and communicate them clearly to individuals.
- **Special Category Data** - Sensitive data requiring extra protection (e.g., health information).

8. Data Lifecycle

Personal data within the society follows a simple lifecycle:

- Collection (e.g., membership forms)
- Storage (digital or paper)
- Access (restricted to authorised roles)
- Use (membership administration and society activities)
- Sharing (only where lawful and necessary)
- Retention (for defined periods)
- Deletion (securely and promptly)

Understanding this lifecycle helps ensure consistent, compliant handling of data at every stage.

9. Common Misunderstandings

Several misconceptions frequently arise when societies begin working with UK GDPR. Addressing them early helps committees focus on what is genuinely required and avoid unnecessary or overly burdensome practices.

- **Consent is not required for most membership communications.**
  Routine emails about meetings, events, newsletters, and membership administration are covered under the lawful basis of Contract. Consent is only needed for optional activities such as marketing to non-members or DBS checks.

- **Small societies do not need to appoint both a Data Controller and a Data Processor**.
  For most astronomy groups, the society itself is the Data Controller, and external service providers (e.g., cloud storage platforms) act as Data Processors. A single Data Protection Lead is usually sufficient to oversee compliance.

- **GDPR does not prevent societies from emailing their members.**
  It requires a lawful basis and secure handling, not silence. Using BCC and maintaining accurate records is usually enough.

- **You do not need to collect more data "just in case."**
  GDPR requires data minimisation. Only collect what is necessary to run the society safely and effectively.

- **Using cloud services is not prohibited.**
  Reputable cloud platforms (e.g., Microsoft 365, Google Workspace) are fully compatible

with GDPR when used securely and with appropriate access controls.

- **GDPR does not require expensive software or consultants.**
  Most compliance steps—clear communication, secure storage, limited access, and timely deletion—are straightforward and low-cost.

- **A data breach does not automatically mean a fine.**
  What matters is how the society responds: assessing the risk, notifying the ICO when required, informing affected individuals, and documenting the incident.

10. Practical Examples of Good and Poor Practice

Emailing members

- **Good:** Using BCC for group messages; sending from a committee-managed email account with 2FA.
- **Poor:** Using CC; sending from a personal email account with weak security.

Sign-in sheets

- **Good:** Recording only name and time of arrival; storing the sheet securely after the event.
- **Poor:** Leaving the sheet unattended; asking for unnecessary details such as full address.

Data minimisation

- **Good:** Asking "Are you over 18?" when age verification is required.
- **Poor:** Collecting full dates of birth without a clear purpose.

Access control

- **Good:** Restricting membership list access to the Membership Secretary and Chair.
- **Poor:** Storing the membership list in a shared folder accessible to all volunteers.

Cloud storage

- **Good:** Using Microsoft 365 or Google Workspace with role-based access.
- **Poor:** Storing personal data on unencrypted USB sticks or personal devices.

11. The Five Core Duties

Every astronomical society must meet five essential obligations.

1. Identify the lawful basis for each activity

Most membership activities rely on Contract, while Gift Aid uses Legal Obligation, and DBS checks require Consent.

2. Minimise the data you collect

Collect only what is necessary. For example, ask "Are you over 18?" rather than requesting a full date of birth.

3. Secure all personal data

Use password protection, encryption, secure cloud storage, and locked cabinets.

4. Appoint a Data Protection Lead

A committee member should oversee compliance, respond to requests, and maintain documentation.

Data Protection Lead – Role Description

The Data Protection Lead (DPL) is a committee member responsible for coordinating GDPR compliance. This is not a legal or technical role; it is an administrative and oversight function.

Responsibilities include:

- Maintaining the Data Audit, ROPA, and Retention Schedule
- Coordinating responses to Subject Access Requests
- Keeping the Privacy Notice up to date
- Advising the committee on data protection matters
- Recording and investigating data breaches
- Ensuring access permissions are reviewed annually

The DPL is not responsible for:

- Personally guaranteeing compliance
- Acting as a legal adviser
- Managing all society data themselves

Time commitment:

- Typically 2–4 hours per month
- Plus an annual review.

5. Be transparent

Provide a clear Privacy Notice on your website and membership forms.

12. Lawful Bases for Processing

Each processing activity must have a lawful basis. The most relevant for astronomical societies are:

1. Contract

Used for:

- Maintaining membership lists
- Sending newsletters and event information

- Providing access to meetings, observing sessions, or members-only areas

Communications that are necessary to deliver membership benefits—such as newsletters, meeting notices, event updates, and administrative messages—are covered under the lawful basis of Contract and do not require separate consent.

2. Legal Obligation

Used for:

- Gift Aid submissions to HMRC
- Statutory financial record-keeping
- Cooperation with law enforcement

3. Consent

Used for:

- DBS checks for volunteers
- Optional marketing communications
- Storing optional health information (e.g., epilepsy disclosure for safety)

4. Legitimate Interests

Used for:

- Observatory sign-in books
- Visitor logs for health & safety
- CCTV where applicable

When relying on Legitimate Interests, the society must ensure that the purpose is reasonable, that the impact on individuals is minimal, and that the society's interests do not override the rights and freedoms of the people whose data is being processed. This is known as the "balancing test."

13. Legitimate Interests Assessment (LIA)

Purpose Test – What are we trying to achieve?

Describe the activity (e.g., visitor log, CCTV, observatory access records) and why it is necessary.

Necessity Test – Is this the least intrusive way?

Explain why the activity is needed and whether alternatives exist.

Balancing Test – Impact on individuals

Consider:

- Would people expect this processing?
- Is the data low-risk?
- Can individuals opt out?

- Are safeguards in place?

Outcome:

☐ Legitimate Interests is appropriate
☐ Additional safeguards required
☐ Do not proceed

Signed:
Date:

14. Member Rights

Societies must be able to respond within one calendar month to:

- Right of Access
- Right to Rectification
- Right to Erasure
  NB Right to Erasure" does not apply to data the society is legally required to keep, such as Gift Aid declarations (6 years) or accident reports (3+ years)
- Right to Restrict Processing
- Right to Object
- Right to be Informed
- Right to Data Portability: Members can ask for a digital copy of their data to move to another society.
  Proportionate Tip: For most societies, simply emailing the member their details in an Excel or CSV file satisfies this right. It only applies to data held electronically.

15. Subject Access Request (SAR) Workflow and Template

Subject Access Request (SAR) Workflow

1. **Receive request**

   - Remember a request can be made verbally or via social media. It does not have to in writing although having it in writing means it is clear what has been ask for. If necessary, clarify what is being asked for. Requests do not need to mention "GDPR" or "Subject Access Request" to be legally valid.
   - Verify identity if needed.
   - Log the request.

2. **Locate data**

   Search:

   - Membership records
   - Emails

- Cloud storage
- Event logs
- Financial records

3. **Review data**

   - Remove third-party data
   - Remove legally privileged information
   - Redact sensitive data where appropriate

4. **Respond within one calendar month**

   Provide:

   - Copy of personal data
   - Explanation of how it is used
   - Lawful basis
   - Retention periods
   - Rights of the individual

5. **Record completion**

   Update the SAR log.

SAR Response Template

Dear [Name],

Thank you for your request of [date].

We have provided the personal data we hold about you, along with information about how it is used, our lawful basis for processing, and your rights under UK GDPR.

If you believe any information is inaccurate or incomplete, please let us know.

Kind regards,
Data Protection Lead
[Society Name]

16. Data Minimisation And Retention

Collect only what you need

Avoid collecting:

- Full dates of birth
- Sensitive data (ethnicity, religion, health) unless volunteered for safety

Retention periods

- Membership data: retained only while the person is a member
- Gift Aid: 6 years (HMRC requirement)
- Visitor logs: 1 year unless an incident occurs

- Accident reports: 3 years (adults) or until a child turns 21

Delete data at the earliest appropriate opportunity.

17. Consolidated Retention Schedule

Retention Schedule (Summary Table)

Data Type	Retention Period	Notes
Membership records	Duration of membership	Delete promptly when membership lapses.
Gift Aid declarations	6 years after relevant accounting period	HMRC requirement.
Financial records containing personal data	6 years	Applies to invoices, receipts, bank statements.
Visitor and event logs	1 year	Longer if an incident occurs.
Accident/incident reports (adults)	3 years	Legal requirement.
Accident/incident reports (children)	Until the child turns 21	Legal requirement.
DBS check outcome	Until suitability decision is made	Do not retain certificates.
Website contact form submissions	6 months	Longer if correspondence continues.
Loaned equipment records	Until equipment is returned	Delete immediately afterwards.
CCTV footage (if used)	30 days	Unless required for an investigation.
Committee minutes	Permanently	Redact sensitive personal data.
Emails containing personal data	As short as possible	Move to secure storage if needed for record-keeping.
Historical Membership Records (Name and Years only)	Permanent.	Retain for heritage purposes; remove all contact details

18. Data Security

Digital security

- Password-protect all files containing personal data
- Encrypt laptops and portable devices
- Use secure cloud storage with 2FA
- Use BCC for group emails (email addresses are personal data and must not be shared inadvertently).

Digital Handover Protocol.

When a committee member stands down, they should certify they have transferred society data to the new officer and deleted local copies.

International Data Transfers

Most reputable cloud providers store data within the UK or EEA, or in countries with adequate data protection laws. Where data is stored outside the UK, providers must offer appropriate safeguards such as Standard Contractual Clauses. Societies should check their provider's privacy policy to confirm where data is stored and ensure appropriate protections are in place.

Paper security

- Store in locked cabinets
- Use cross-cut shredders for disposal
- Legacy Archives. Conduct a "Archive Audit" to shred old membership forms or bank statements while keeping the actual minute books

Access control

- Limit access to those who genuinely need it
- Remove access when roles change

19. Minimum Technical Standards

These standards help ensure proportionate, practical security for volunteer-run societies.

- Strong passwords (minimum 12 characters)
- Two-factor authentication on all committee accounts
- No shared logins
- Encrypted laptops or devices storing personal data
- Cloud storage with access-controlled folders
- Regular deletion of old emails
- No personal data stored on USB sticks
- Ensure all devices used for society business (laptops, tablets, phones) have automatic software updates enabled for both the Operating System and security software
- Committee email accounts separate from personal accounts where practicable

20. Data Breach Protocol

A personal data breach includes, but is not limited to:

- Lost or stolen laptop/USB stick
- Email sent using CC instead of BCC
- Lost printed membership list
- Hacked email account
- Accidental deletion of data without backup

If a breach occurs

1. Assess the risk immediately
2. Report to the ICO within 72 hours if there is any risk to individuals
3. Notify affected members
4. Investigate and document the incident

5. Report findings within 28 days

21. Data Breach Decision Tree

1. Has personal data been lost, accessed, altered, or shared without permission?

- If no → Not a breach. Record if uncertain.
- If yes → Continue.

2. What type of data is involved?

- Contact details
- Membership data
- Special category data
- Children's data

3. What is the risk to individuals?

- Could it cause harm, distress, or inconvenience?
- Could it expose someone's identity or location?
- Could it lead to fraud or impersonation?

4. Is there any risk to individuals?

- If yes → Notify ICO within 72 hours.
- If no → Record in breach log.

5. Do individuals need to be informed?

- If they need to take action to protect themselves → Yes.
- If risk is minimal → No.

6. Record everything

- What happened
- What data was involved
- Who was affected
- Actions taken
- Lessons learned

22. Special Considerations

Children and young people

- Children aged 13+ can consent to online services
- Under 13 requires parental consent
- Privacy notices must pass the "child test"—in other words, be clearly understood by a child.

Health disclosures

If a member voluntarily shares health information (e.g., epilepsy), record only what is necessary and agree who may access it.

Visitors and public events

Collect only minimal data and delete promptly unless an incident occurs.

Historical Archiving

Many astronomical societies take pride in their heritage and may wish to keep member lists or meeting minutes for decades. While most data should be deleted, societies can retain minimal records (like name and years of membership) for historical archives, provided they are stored securely and the "Right to Erasure" is balanced against the "Public Interest" of historical record-keeping.

Photography and Filming at Events

Photography and video recording at society events may involve personal data if individuals can be identified. The lawful basis depends on the context and expectations of attendees.

General event photography (Legitimate Interests):

- Appropriate for wide-angle shots of events where photography is expected.
- Provide clear signage stating that photography may take place.
- Avoid capturing individuals who have opted out.

Close-ups, posed photos, or identifiable images of individuals (Consent):

- Obtain explicit consent before taking or publishing identifiable images.
- Keep a record of consent and allow individuals to withdraw it at any time.

Children and young people:

- Always obtain parental consent for identifiable images.
- Avoid publishing children's images on public platforms unless strictly necessary and consent is clear.

Good practice:

- Offer a simple opt-out method (e.g., a discreet badge or wristband).
- Avoid publishing images that could cause embarrassment or risk.
- Store images securely and delete those no longer needed.

Personal photography by individual members for their own private use (e.g., a member taking a photo of their friend at a telescope) generally falls under the "personal or household activities" exemption and is not the society's responsibility under UK GDPR, provided the society didn't facilitate or publish the image.

CCTV

If using fixed CCTV, a sign must be clearly displayed at the entrance to the monitored area, stating that CCTV is in operation, the purpose (e.g., security), and who to contact (the DPL).

Informal Communication Channels

- Ensure members "Opt-In" specifically for group chats where their number will be visible to others.
- Remind moderators to remove former members promptly to align with the retention schedule

Loaned equipment

Retain contact details until equipment is returned.

Unincorporated societies

Committee members may be personally liable for fines or legal costs arising from a data breach."

23. Additional Considerations for Charitable Astronomical Societies

(Applies only to registered charities or societies applying for charitable status.)

Gift Aid and HMRC Compliance

Charities must:

- Retain Gift Aid declarations for 6 years
- Keep auditable donation records
- Restrict access to Gift Aid data
- Ensure secure storage and backups

Charity Commission Expectations

Trustees must demonstrate:

- Good governance of personal data
- Clear accountability
- Documented risk management
- Evidence of annual review

Higher Liability for Trustees

Trustees may be held accountable for governance failures even without an ICO fine.

Fundraising and Supporter Data

- Marketing to non-members requires Consent
- Donor data must be minimised

- Fundraising platforms require Data Processing Agreements

Volunteer Management and DBS Checks

- DBS checks require explicit Consent
- Results must not be retained longer than necessary

Safeguarding Records

- Strict access controls
- Longer retention periods
- Clear documentation

Reporting Serious Incidents

Charities must report serious breaches to:

1. The ICO
2. The Charity Commission

24. Guidance on Committee Minutes

Committee Minutes and Personal Data

Committee minutes often contain personal data. To remain compliant:

- Record only what is necessary
- Avoid including sensitive personal data unless essential
- Store minutes securely in a controlled-access folder
- Redact personal data before publishing minutes to members
- Keep minutes permanently as part of the society's governance record
- Record safeguarding matters in a separate confidential log

25. Data Sharing with Partner Organisations

Any sharing with schools, councils, museums, or grant bodies requires:

- A lawful basis
- A written Data Sharing Agreement
- Assurance of GDPR compliance

26. Data Processing Agreement Checklist

Use this checklist when working with any external provider that processes personal data on behalf of the society (e.g., cloud storage, mailing lists, ticketing platforms).
Societies must remember that they are the Data Controller for the information downloaded from these sites and must ensure they only download what is necessary (data minimisation) and delete the local copies according to their retention schedule.

A compliant provider should confirm:

- They only process data on your documented instructions
- They have appropriate security measures in place
- They ensure confidentiality of staff handling your data
- They assist with data breach notifications
- They assist with Subject Access Requests
- They delete or return data at the end of the contract
- They allow audits or provide compliance reports
- They use sub-processors only with your knowledge
- They store data in the UK or in countries with adequate protection

Keep a copy of the provider's privacy policy and contract.

27. Annual Compliance Checklist

- Review membership data accuracy
- Delete data for former members
- Review access permissions
- Test backups
- Review Privacy Notice
- Review breach log
- Confirm DPL role
- Confirm that responsibilities are clearly defined for any ongoing joint events with external partner(s)
- Review retention schedule

28. Annual GDPR Review Template

1. Membership Data

- Is the membership list accurate and up to date?
- Have former members' data been deleted?
- Are any legacy spreadsheets or backups still stored unnecessarily?

2. Access Permissions

- Are access rights still appropriate for each committee role?
- Have permissions been removed for former officers and volunteers?

3. Privacy Notice

- Has the Privacy Notice been reviewed and updated if needed?
- Is it published on the website and included with membership forms?

4. Retention Schedule

- Have expired records been deleted?
- Are any retention periods unclear or needing revision?

5. Data Breach Log

- Have any breaches occurred this year?

- Were they investigated and documented?
- Have lessons learned been implemented?

6. Technical Security

- Are committee devices encrypted?
- Is two-factor authentication enabled on all accounts?
- Are shared logins avoided?
- Are backups tested and working?

7. Documentation

- Has the Data Audit been updated?
- Has the ROPA been reviewed?
- Are Data Processing Agreements current and complete?

8. Training and Awareness

- Have new committee members received a GDPR briefing?
- Are volunteers aware of basic data handling expectations?

Signed:

Date:

Next review due:

Appendix A — Privacy Notice Template

Privacy Notice for [Society Name]

We collect and process personal data to administer your membership, provide society services, and meet our legal obligations.

What we collect:

Name, contact details, membership status, payment records, Gift Aid declarations (if applicable).

Lawful bases:

Contract (membership administration), Legal Obligation (Gift Aid), Consent (optional activities), Legitimate Interests (health & safety logs).

How we use your data:

To send newsletters, event information, manage meetings, maintain membership records, and comply with HMRC requirements.

How long we keep your data:

Membership data is deleted when you leave the society unless legally required for longer. While we delete most data when you leave, we may retain a minimal record (your name and years of membership) in our historical archives to preserve the society's heritage and record of astronomical contributions

Your rights:

You may request access, correction, deletion, or restriction of your data.

Contact:

Data Protection Lead: [Name] – [Email]

Appendix B — Data Audit Template

1. **Data Collected**

   (e.g., name, email, phone number, Gift Aid status)

2. **Purpose**

   (e.g., membership administration, event communication)

3. **Lawful Basis**

   (Contract / Legal Obligation / Consent / Legitimate Interests)

4. **Storage Location**

   (e.g., encrypted laptop, cloud drive)

5. **Access**

   (roles with access)

6. **Retention Period**

7. **Risks and Controls**

Appendix C — Record of Processing Activities (ROPA)

Membership Administration

Processing Activity	Membership administration
Data Types	Name, postal address, email address, phone number, membership status, payment records
Lawful Basis	Contract
Storage Location	Secure cloud drive (Microsoft 365 or Google Workspace)
Retention Period	Duration of membership
Security Measures	Password protection; two-factor authentication; restricted committee access

Historical Society Archives

Processing Activity	Maintenance of Historical Society Archives
Data Types	Name of member; years of membership; roles held (e.g., Committee Officer); notable astronomical contributions or awards
Lawful Basis	Legitimate Interests: To preserve the heritage, history, and scientific contributions of the society
Storage Location	Secure digital archive folder or locked physical archive box
Retention Period	Permanent: Retained as a core part of the society's historical record
Security Measures	Data minimisation (removal of contact details/addresses); restricted access to authorized archive officers; password protection for digital files

Gift Aid Administration

Processing Activity	Gift Aid administration
Data Types	Name, postal address, taxpayer status, Gift Aid declaration
Lawful Basis	Legal Obligation
Storage Location	Treasurer's secure records (digital or paper)
Retention Period	Six years after the end of the relevant accounting period
Security Measures	Encrypted digital storage or locked filing cabinet; restricted access

DBS Checks for Volunteers

Processing Activity	DBS checks for volunteers
Data Types	Identity documents; DBS application details; confirmation of outcome
Lawful Basis	Consent
Storage Location	Secure digital folder or locked cabinet
Retention Period	Only until the suitability decision is made; DBS certificates must not be retained
Security Measures	Strict access control; minimal data retention

Visitor and Event Sign-In Logs

Processing Activity	Visitor and event sign-in logs
Data Types	Name; contact details; date/time of visit
Lawful Basis	Legitimate Interests (health and safety)
Storage Location	Paper logbook or secure digital file
Retention Period	One year unless an incident requires longer retention
Security Measures	Locked storage for paper logs; restricted access for digital logs

Accident and Incident Reporting

Processing Activity	Accident and incident reporting
Data Types	Name; contact details; description of incident; witness details
Lawful Basis	Legal Obligation (health and safety)
Storage Location	Secure digital folder or locked cabinet
Retention Period	Three years for adults; until age 21 for incidents involving children
Security Measures	Restricted access; encrypted storage or locked filing cabinet

Email Communications to Members

Processing Activity	Email communications to members
Data Types	Email address; name
Lawful Basis	Contract
Storage Location	Society email account or mailing list system
Retention Period	Duration of membership
Security Measures	Use of BCC for group emails; secure email account with strong password and two-factor authentication

Website Contact Form Submissions

Processing Activity	Website contact form submissions
Data Types	Name; email address; message content
Lawful Basis	Legitimate Interests (responding to enquiries)
Storage Location	Website CMS or society email inbox
Retention Period	Six months unless further correspondence requires longer
Security Measures	Secure website hosting; password-protected email account

Loaned Equipment Tracking

Processing Activity	Loaned equipment tracking
Data Types	Name; contact details; equipment details; loan dates
Lawful Basis	Contract (fulfilling membership services)
Storage Location	Secure digital file
Retention Period	Until equipment is returned
Security Measures	Restricted access; password-protected file

Appendix D — Data Breach Response Log

- Date and time of breach
- Description of incident
- Data involved
- Risk assessment
- ICO notification (yes/no)
- Member notification (yes/no)
- Corrective actions
- Lessons learned

This log should be reviewed annually by the committee, even if no breaches have occurred.