chamboree

DATA PROTECTION & INFORMATION HANDLING POLICY

Applies to: All participants, leaders, International Service Team (IST) members, contractors, visitors and external partners.

1. Purpose of This Policy

Chamboree collects, stores and processes personal information about participants, leaders, volunteers, staff, contractors and visitors to ensure the safe and effective delivery of the event.

This policy sets out:

- What personal data is collected
- How data is processed, shared, stored and protected
- Roles and responsibilities for handling data
- Expected standards of behaviour
- Requirements under UK GDPR and the Data Protection Act 2018
- How to respond to data incidents or breaches
- Data retention and deletion requirements

This policy ensures that data is used lawfully, fairly, securely and transparently.

This policy must be read alongside the Photography, Video & Social Media Policy for all matters relating to media capture and usage.

2. Scope

This policy applies to:

- All event staff, leaders and volunteers
- All contractors and external providers handling event data
- All directorates and sub-teams
- Any individual accessing event systems
- All paper and digital data processed before, during and after the event

This includes personal data such as:

- Participant and staff details
- Medical and welfare information
- Safeguarding records
- Contact details for emergency use
- Photos, video and audio recordings
- Operational records (e.g. incident logs, rosters)

Sensitive personal data (e.g. medical, safeguarding, accessibility needs) is subject to stricter controls. Much of the data processed relates to young people and must be handled with additional care and safeguarding consideration.

3. Legal Framework

Chamboree processes personal data in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- The Scouts and Girlguiding policies
- Safeguarding and duty of care requirements
- Contractual obligations relating to event delivery

Chamboree may act as:

- **Data Processor** on behalf of The Scouts and Girlguiding
- **Data Controller** for event-specific operational data

4. Data Protection Principles

All personal data must be:

- Lawful, fair and transparent
- Used only for specific event purposes
- Limited to what is necessary

- Accurate and up to date
- Retained only as long as required
- Kept secure and confidential
- Handled in a way that demonstrates accountability

5. Categories of Data Collected

5.1 Participant Data
- Name, date of birth and contact details
- Emergency contacts
- Medical conditions, medication and allergies
- Dietary and accessibility needs
- Relevant safeguarding information

5.2 Leader & Staff Data
- Personal and contact details
- Role and qualifications
- DBS/vetting confirmation
- Next of kin information
- Relevant medical or dietary needs

5.3 Operational Data
- Incident records
- Access logs
- Shift rosters
- Subcamp allocations

5.4 Media Data
- Photos, video and audio recordings
- Consent and opt-out records

6. Use of Data
Personal data may be used for:
- Participant safety and welfare
- Medical treatment and emergency response
- Safeguarding processes
- Programme and subcamp allocation
- Staff rostering and operational coordination
- Communication with leaders and parents/carers
- Accessibility planning
- Compliance with legal obligations

Personal data is **not used for marketing without explicit consent**.
Individuals have rights under UK GDPR including access, correction, deletion, restriction and objection. Requests must be referred to the Data Protection Lead.

7. Data Access & Permissions

7.1 Need-to-Know Basis
Access is strictly limited to those who require information for their role.
Examples:
- Medical Team – medical data
- Safeguarding Team – safeguarding records
- Welfare Team – welfare information
- Subcamp Teams – group allocations and emergency contacts
- Programme Teams – accessibility information

7.2 Access Restrictions
The following must not access sensitive data unless authorised:
- Participants
- Young leaders
- General volunteers not in relevant roles
- External vendors

Access to data may be logged and monitored.

8. Data Storage
8.1 Digital Data
Digital data must:
- Be stored on secure, password-protected systems
- Be encrypted where possible
- Be accessed only by authorised users
- Not be stored on personal devices unless explicitly authorised and secured

Where temporary access via mobile devices is necessary:
- Devices must be password protected
- Devices must not be shared
- Screens must be locked when unattended

8.2 Paper Records
Where paper records are used:
- They must be stored securely when not in use
- They must not be left unattended
- They must be transported discreetly
- They must be returned to the Data Protection Lead after use

9. Data Sharing

9.1 Internal Sharing
Permitted where necessary for operational purposes between:
- Medical, Safeguarding and Welfare Teams
- Subcamp Teams
- Event leadership teams

9.2 External Sharing
Permitted only where lawful and necessary, including:
- Emergency services
- Medical professionals
- Local authority safeguarding teams
- Parents or guardians (where appropriate)
- The Scouts or Girlguiding for escalation

Data must not be shared with:
- Media
- Other participants
- External traders
- Other groups or parents unless required.

Approved third-party providers may access data where necessary to support event delivery and must comply with data protection requirements.
Chamboree does not sell personal data under any circumstances.

10. Photography, Video & Media Data

All media must comply with the **Photography, Video & Media Policy**.
Key principles:

- Respect photo consent and opt-out preferences
- Do not take images of young people outside your responsibility without permission
- Do not attach identifying information without consent
- Do not share images in breach of policy

11. Retention & Deletion of Data
Data will be retained only as long as necessary:

- Standard participant data: **deleted within 3–6 months post-event**
- Medical data: **retained temporarily and then securely destroyed**
- Safeguarding data: **transferred and retained in accordance with national policy**
- Financial data: **retained for audit and legal requirements**
- Security logs: retained in line with legal obligations

All data must be securely deleted or destroyed when no longer required.

12. Data Breaches & Incident Management
A data breach includes:

- Lost or stolen devices
- Unauthorised access or disclosure
- Misdirected communication
- Loss of paper records
- System compromise

12.1 Immediate Actions
Anyone identifying a breach must:

- Report immediately to the **Data Protection Lead (DPL)**
- Inform the **Duty ELT Member/Camp Chief**
- Contain the issue where safe to do so
- Not attempt to resolve it independently

12.2 Response & Investigation
The Data Protection Lead will:

- Assess the severity of the breach
- Escalate to Safeguarding or Medical Teams if required
- Determine whether individuals must be informed
- Report to relevant national organisations
- Notify the ICO if required
- Implement corrective actions

13. Responsibilities of Staff and Volunteers
All individuals handling data must:

- Treat data confidentially
- Only access data required for their role
- Not share data inappropriately
- Secure devices and documents
- Report concerns or incidents immediately
- Comply with this policy at all times

Failure to comply may result in removal from the event or further action.

14. Training Requirements
The following must be completed:

- Data protection awareness for all staff and volunteers
- Additional guidance for roles handling sensitive data
- Briefings for Subcamp, Welfare and operational leaders

- Specialist training for Medical and Safeguarding Teams

15. Authority & Escalation

The Camp Chief retains overall accountability for information governance at Chamboree, supported by the Event Leadership Team.

Significant data protection incidents, breaches or concerns must be escalated promptly to the relevant Event Leadership Team member and managed in accordance with the Event Governance & Roles Policy.

The Duty Manager should be informed where operational action or incident coordination is required.

Document title	Issue number	Date issued	Authorised
Data Protection & Information Handling	1	June 2026	Dave Hopley