Activity Junction LTD

GDPR & Data Protection Policy

Activity Junction reviews all policies on a regular basis to demonstrate good practice, regulations and legislation changes as required.

1. Policy Statement

Activity Junction Ltd is committed to protecting the privacy and personal data of all individuals we interact with, including children, young people, vulnerable adults, parents, carers, staff, and external partners. We collect and process personal information in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy outlines how we manage personal data lawfully, fairly, and transparently.

2. Purpose of the Policy

This policy aims to:

- Ensure all personal data is handled responsibly and securely.
- Set out how we comply with UK GDPR principles.
- Protect the rights and freedoms of data subjects.
- Outline procedures for data access, correction, and deletion.

3. Scope

This policy applies to:

- All staff, volunteers, and contractors at Activity Junction Ltd.
- All personal data processed in relation to our services, activities, and events.
- Data belonging to children, parents/carers, vulnerable adults, staff, and third parties.

4. What Is Personal Data?

Personal data includes:

- Names, addresses, phone numbers, email addresses
- Date of birth
- Medical, educational, or support needs
- Attendance and participation records
- Images or video where individuals can be identified
- Emergency contact and safeguarding information

5. Data Protection Principles

We follow the 7 principles of UK GDPR, ensuring personal data is:

1. Lawfully, fairly and transparently processed
2. Collected for specific, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed securely
7. Accountable – we maintain records to demonstrate compliance

6. Lawful Basis for Processing

We collect and process personal data based on one or more of the following lawful bases:

- Consent (e.g. photo permissions)
- Contractual obligation (e.g. service agreements)
- Legal obligation (e.g. safeguarding)
- Vital interests (e.g. medical emergencies)
- Legitimate interests (e.g. internal planning and safety)

7. Consent

Where required (e.g. for photos, newsletters), we will obtain clear, informed consent.

- Consent is optional and can be withdrawn at any time.
- We use child-friendly consent forms where appropriate.
- For under-13s, consent must be given by a parent or guardian.

8. Storing and Securing Data

We take steps to protect data by:

- Storing paper records in locked cabinets
- Using password-protected digital systems
- Restricting access to authorised staff only
- Using secure, encrypted services for cloud storage and email
- Regularly reviewing data security measures

9. Data Sharing

We will only share personal data:

- With relevant authorities in the case of safeguarding or legal requirements
- With explicit consent (e.g. sharing with schools or external support services)
- When necessary to deliver services or ensure safety

We never sell or disclose personal data for marketing or profit.

10. Data Retention

We retain data only for as long as needed for operational, legal, or safeguarding reasons.
Retention periods are regularly reviewed in line with best practices. Once data is no longer needed, it is securely deleted or destroyed.

11. Your Rights

Under GDPR, individuals have the right to:

- Be informed about how their data is used
- Access their personal data
- Correct inaccurate or incomplete data
- Request deletion of their data (in certain cases)
- Restrict or object to data processing
- Data portability (where applicable)

All requests must be made in writing to our Data Protection Lead and will be responded to within one calendar month.

12. Data Breaches

In the event of a data breach:

- It will be investigated immediately and logged
- Affected individuals will be notified if there is a high risk to their rights
- Serious breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours

13. Staff Responsibilities and Training

All staff and volunteers:

- Must complete data protection training
- Are responsible for following this policy at all times
- Must report any data concerns or breaches to management immediately

14. Review

This policy will be reviewed annually or following any major incident or legislative change.

Date of last review: 24th April 2025
Next review due: 24th April 2026

Approved by:
Emma Devine – Director
Activity Junction Ltd