SI

ACTIVITY CAMPS

CONFIDENTIALITY POLICY

ASHVILLE HARROGATE

SI FOUNDATION

1. Policy Statement

Sporting Influence Ltd is committed to protecting the confidentiality, privacy, and integrity of all personal and sensitive information relating to:

- Children and young people
- Parents and guardians
- Employees and volunteers
- Schools and partner organisations
- Business operations

We recognise our obligations under:

- The Data Protection Act 2018
- UK GDPR (General Data Protection Regulation)
- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children

Confidentiality is essential to maintaining trust, safeguarding children, and ensuring professional standards at all times.

2. Scope

This policy applies to:

- All employees (full-time, part-time, casual)
- Freelance coaches and contractors
- Volunteers and work experience students
- Directors and senior management
- Anyone acting on behalf of Sporting Influence Ltd

This policy applies during:

- School delivery
- Activity Camps
- Community sessions
- Remote or home working
- Digital communication

3. Definition of Confidential Information

Confidential information includes (but is not limited to):

3.1 Personal Information

- Names, addresses, contact details
- Dates of birth
- Medical information
- SEN or additional needs information
- Safeguarding records
- Behavioural records

3.2 Employment Information

- Contracts
- Payroll details
- Disciplinary records
- Performance information

3.3 Business Information

- Financial records
- Client agreements
- Pricing structures
- Strategic plans
- Internal communications

3.4 Safeguarding Information

- Child protection concerns
- Disclosures made by children
- Referral documentation
- Agency communications

Safeguarding information is always considered highly confidential.

4. Core Principles

Sporting Influence Ltd operates under the following principles:

- Information is shared on a **need-to-know basis only**.
- Confidential information must be handled securely at all times.
- Safeguarding concerns override general confidentiality where a child is at risk of harm.
- Staff must never promise absolute confidentiality to a child.
- Information must only be shared with appropriate authorities or designated persons.

5. Staff Responsibilities

All staff must:

- Keep all personal and sensitive information secure.
- Not discuss confidential matters in public areas.
- Not access information unless necessary for their role.
- Not share login details or passwords.
- Lock devices when unattended.
- Ensure paper records are stored securely.
- Report data breaches immediately.

Staff must not:

- Share information via personal social media.
- Use personal email accounts for confidential matters.
- Remove sensitive documents from premises unless authorised.
- Discuss children or staff in informal or social settings.

6. Safeguarding & Confidentiality

6.1 Disclosures from Children

If a child makes a disclosure:

- Listen carefully and remain calm.
- Do not promise to keep secrets.
- Explain that information may need to be shared to keep them safe.
- Record the disclosure accurately.
- Report immediately to:
  - The School Designated Safeguarding Lead (DSL), or
  - The Sporting Influence Safeguarding Lead (during camps).

6.2 Information Sharing in Safeguarding

Information may be shared:

- With the DSL
- With local safeguarding authorities
- With police
- With social services

This sharing is lawful and necessary where safeguarding concerns exist.

7. Data Storage & Security

7.1 Electronic Data

- Stored on secure, password-protected systems.
- Access restricted based on role.
- Two-factor authentication used where possible.
- Cloud systems must comply with UK GDPR.

7.2 Paper Records

- Stored in locked cabinets.
- Access limited to authorised personnel.
- Shredded securely when no longer required.

7.3 Portable Devices

- Must be password protected.
- Must not be left unattended in vehicles.
- Loss or theft must be reported immediately.

8. Communication & Confidentiality

8.1 Email

- Only company email accounts to be used.
- Check recipients carefully before sending.
- Use BCC where sending group emails.

8.2 Messaging

- Only approved communication platforms may be used.
- No direct personal messaging with children.
- Parent communication must follow company procedures.

8.3 Meetings

- Confidential matters discussed in private.
- Sensitive conversations not held in open environments.

9. Photography & Media

- Photos or videos of children may only be taken:
  - With parental consent.
  - Using company devices.
- Images must not be stored on personal devices.
- Images must not be shared without authorisation.

10. Data Breaches

A data breach includes:

- Loss of personal data.
- Sending information to the wrong recipient.
- Unauthorised access to records.
- Stolen or lost devices containing personal data.

All data breaches must be:

- Reported immediately to senior management.
- Investigated promptly.
- Reported to the ICO where required under UK GDPR.

Failure to report a breach may result in disciplinary action.

11. Confidentiality After Employment Ends

Confidentiality obligations continue:

- After employment or contract ends.
- Without time limitation regarding safeguarding matters.
- For all business-sensitive information.

Former staff must not retain or use confidential information.

12. Breach of Confidentiality

Failure to comply with this policy may result in:

- Disciplinary action.
- Termination of contract.
- Legal action.
- Referral to regulatory bodies (where applicable).

Serious safeguarding breaches will be treated as gross misconduct.

13. Training

All staff will:

- Receive confidentiality training during induction.
- Complete safeguarding training annually.
- Be informed of updates to data protection law.

14. Policy Review

This policy will be reviewed:

- Annually
- Following legislative updates
- Following any significant data breach
- Following safeguarding incidents

Approval

Approved by: C Doey
Position: Camp Leader
Date: 27/02/2026
Review Date: 27/02/2027