Data Protection & Confidentiality Policy

Approval date: March 2026

Approved by: Board of Trustees

Review date: March 2027

1. Purpose

North Somerset Sports Foundation is committed to protecting personal data and maintaining the confidentiality of all information it handles.

This policy ensures that all personal and sensitive information is processed lawfully, fairly, and securely in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We aim to:

- Protect the privacy of individuals
- Maintain trust and transparency
- Prevent unauthorised access, misuse, or loss of data

2. Scope

This policy applies to:

- Employees, trustees, and volunteers
- Contractors and third-party providers
- All personal data processed by North Somerset Sports Foundation

This includes data held:

- Digitally
- In paper format
- Across all systems and platforms

3. Data Protection Principles

North Somerset Sports Foundation adheres to the seven principles of UK GDPR :

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

4. Data Controller and Responsibility

North Somerset Sports Foundation acts as the Data Controller and is responsible for determining how personal data is processed.

Data Protection Lead

Lucy Chappell (CEO) is Data Protection Lead, and is responsible for overseeing compliance with data protection legislation.

Responsibilities include:
- Managing data protection processes
- Handling Subject Access Requests (SARs)
- Managing data breaches
- Providing guidance and training

5. Lawful Basis for Processing

We will only process personal data where a lawful basis applies, including:
- Consent
- Contractual necessity
- Legal obligation
- Legitimate interests
- Vital interests (where applicable)

Where consent is relied upon, it will be:
- Freely given
- Specific
- Informed
- Capable of being withdrawn

Further detail on how we process personal data is outlined in our Privacy Notice.

6. Privacy Notice

North Somerset Sports Foundation maintains a Privacy Notice which explains:

- What personal data we collect
- How and why it is used
- How long it is retained
- Individual rights

7. Types of Data Held

Personal Data

Includes names, contact details, and identifying information.

Special Category Data

Includes:
- Health information
- Safeguarding-related data
- Equality and diversity data
- This data is subject to additional safeguards and restricted access.

Children's Data

We recognise that children's data requires a higher level of protection.

North Somerset Sports Foundation will:
- Process children's data lawfully and transparently
- Ensure appropriate consent is obtained where required
- Limit access to authorised individuals only
- Handle safeguarding-related data with particular care

8. Individual Rights

Individuals have the following rights under UK GDPR:
- The right to be informed
- The right of access (Subject Access Request – SAR)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

Subject Access Requests (SARs)
- Requests must be responded to within one month
- No fee will normally be charged
- Requests should be directed to the Data Protection Lead

9. Data Storage and Security

We will ensure that:
- Personal data is stored securely
- Digital data is protected through passwords, encryption, and access controls
- Physical records are stored in locked and secure locations
- Access is restricted to authorised individuals only

Staff and volunteers must:
- Only access data necessary for their role
- Avoid using unsecured systems or personal devices for sensitive data
- Ensure conversations involving personal data are conducted privately

10. Data Retention

Personal data will only be retained for as long as necessary to fulfil its purpose.

North Somerset Sports Foundation will:

- Maintain a data retention schedule
- Regularly review stored data
- Securely delete or destroy data when no longer required

11. Data Records and Accountability

North Somerset Sports Foundation maintains a central record of data processing activities (ROPA).

This record includes:

- Categories of personal data processed
- Purpose of processing
- Lawful basis
- Data retention periods
- Data sharing arrangements
- This supports compliance with UK GDPR accountability requirements.

12. Data Sharing and Third Parties

Personal data will only be shared:

- Where there is a lawful basis
- With appropriate safeguards in place

All third parties must:

- Comply with UK GDPR
- Have appropriate data processing agreements in place
- Demonstrate adequate security measures
- Data will be anonymised where possible before sharing.

13. Data Breaches

A data breach includes any loss, unauthorised access, or disclosure of personal data.
All staff and volunteers must report suspected breaches immediately to the Data Protection Lead.

Breach Management

The Data Protection Lead is responsible for:

- Assessing the severity of the breach
- Coordinating the response
- Determining whether the breach is reportable

Where required, North Somerset Sports Foundation will:

- Notify the Information Commissioner's Office (ICO) within 72 hours
- Inform affected individuals where there is a high risk

14. Confidentiality

All staff, volunteers, and stakeholders must maintain confidentiality at all times.

Confidential information must not be:

- Shared without authorisation
- Discussed in public or insecure environments
- Used outside legitimate organisational activity

15. Monitoring and Review

- Compliance will be monitored regularly
- Training will be provided as required
- This policy will be reviewed annually or following significant changes

16. Contact and Complaints

Any questions or concerns regarding data protection should be directed to:

- The Data Protection Lead
- Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO).

17. Conclusion

North Somerset Sports Foundation is committed to maintaining the highest standards of data protection and confidentiality.
Through clear accountability, secure handling of data, and compliance with legal requirements, we aim to maintain a safe and trustworthy environment for all.