STOOLBALL ENGLAND

STORAGE, HANDLING, USE, RETENTION AND DISPOSAL OF DISCLOSURE INFORMATION

POLICY AND PROCEDURE (2026 MASTER VERSION)

Organisation: Stoolball England
Applicable to: Stoolball England Volunteer Workforce, including freelance and self-employed coaches
Effective From: January 2026
Policy Owner: Safeguarding & Welfare Lead / Data Protection Lead
Approved By: Board
Approval Date: January 2026
Version: 1.0 (2026 Governance Suite)
Next Review: January 2027
Review Cycle: Annual

1. POLICY STATEMENT

Stoolball England recognises its legal and ethical responsibility to handle criminal record disclosure information in a fair, lawful and secure manner.

This policy sets out how Disclosure and Barring Service (DBS) information is stored, handled, used, retained and disposed of in compliance with:

- DBS Code of Practice
- UK GDPR
- Data Protection Act 2018
- Police Act 1997

This policy applies to all DBS information relating to volunteers, freelance or self-employed coaches, and any other individual engaged by Stoolball England.

Unauthorised disclosure of DBS information is a criminal offence.

2. LEGAL FRAMEWORK

This policy is informed by and complies with:

- DBS Code of Practice
- Police Act 1997 (sections relating to disclosure information)
- UK GDPR
- Data Protection Act 2018
- Human Rights Act 1998

3. STORAGE OF DISCLOSURE INFORMATION

3.1 Physical Storage

Any paper-based disclosure information will be:

- Stored in locked, non-portable storage
- Kept separately from general personnel or volunteer files
- Accessible only to authorised individuals

3.2 Digital Storage

Where disclosure information is stored electronically:

- Files will be encrypted and password-protected
- Access will be restricted to named authorised officers
- Systems will comply with Stoolball England's data security controls

DBS certificates themselves will not be scanned, uploaded or stored electronically.

4. HANDLING OF DISCLOSURE INFORMATION

- Disclosure information will only be handled by individuals authorised as part of their role.
- Information will not be shared with anyone who is not entitled to see it.
- A record will be kept of:
    - Who accessed the information
    - The date and purpose of access

Disclosure information must never be discussed informally or outside the recruitment or safeguarding decision-making process.

5. USE OF DISCLOSURE INFORMATION

Disclosure information will only be used:

- For the specific purpose for which it was requested
- To assess suitability for a role or safeguarding decision

Information will not be used for any other purpose or retained for future recruitment decisions.

6. RETENTION OF DISCLOSURE INFORMATION

Stoolball England will not retain disclosure information for longer than is necessary.

In most cases:

- Information will be retained for no longer than six months following a recruitment or engagement decision.

Longer retention will only occur where:

- A safeguarding concern is ongoing
- There is a legal or regulatory requirement

Any extended retention must be documented and justified.

7. DISPOSAL OF DISCLOSURE INFORMATION

Once the retention period has expired, disclosure information will be securely destroyed by:

- Shredding
- Pulping
- Secure electronic deletion

No copies, scans or extracts of DBS certificates will be retained.

8. THIRD-PARTY AND UMBRELLA BODY PROCESSING

Stoolball England works with approved DBS umbrella bodies and third-party processors.

Contracts and agreements will ensure:

- Compliance with the DBS Code of Practice
- Compliance with UK GDPR
- Clear responsibilities for secure handling and disposal

9. ROLES AND RESPONSIBILITIES

Safeguarding & Welfare Lead
Responsible for authorisation of access to disclosure information and safeguarding decisions arising from DBS checks.

Data Protection Lead
Responsible for data protection compliance, security controls and lawful processing of disclosure information.

Recruiters / Managers
Responsible for ensuring adherence to this policy during recruitment and engagement processes.

10. MONITORING AND REVIEW

Compliance with this policy will be monitored through:

- Safeguarding audits
- Club compliance checks

- Incident or case reviews

This policy will be reviewed annually or sooner if legislation or DBS guidance changes.

DOCUMENT CONTROL

Version: 1.0
Suite: 2026 Governance & Safeguarding Framework
Status: Approved
Owner: Safeguarding & Welfare Lead / Data Protection Lead
Next Scheduled Review: January 2027

VERIFICATION STATEMENT

This document has been reviewed against the DBS Code of Practice and relevant legislation and is verified as complete, internally consistent and suitable for formal publication as part of the 2026 Governance Suite.