Procedure Number:	08
Version:	2025.09
Release Date:	01/09/2025
Review Date:	

Durham & Northumberland Archery Association

Data Protection & Handling Policy Framework

1. Policy Statement

1.1. DNAA is committed to handling all personal and special-category data in a lawful, transparent, and secure manner. This policy MUST be followed by all **Users** — defined as *any person who collects, stores, uses, shares, or disposes of DNAA data (physical or electronic), whether in a formal role, voluntary capacity, or third-party position acting on DNAA's behalf*. This includes (but is not limited to): officers, coaches, committee members, event organisers, volunteers, and contracted processors.

1.2. **Good Practice:** Keep a clear, concise summary of this statement available to all volunteers to reinforce shared commitment.

2. How to Use This Policy

2.1. This policy uses two defined terms to indicate the priority of requirements:

2.1.1. MUST – a mandatory requirement. Failure to comply is a breach of this policy and may constitute non-compliance with UK GDPR and the Data Protection Act 2018.

2.1.2. SHOULD – a strongly recommended practice. Deviation is permitted only if you document a justified reason.

2.1.3. Legal and technical terms have been minimised. Whenever you see a term in *italics*, its precise meaning can be found in Section 4 (Definitions).

2.2. 2.3 If you are ever uncertain how to proceed, follow the nearest MUST clause or consult the Data Protection Lead for guidance.

3. Purpose

3.1. Establish a clear, consistent approach to data protection across all DNAA operations and affiliated clubs.

3.2. Ensure full compliance with applicable legislation — including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and requirements set by Archery GB.

3.3. Protect the rights, freedoms, and personal data of individuals entrusted to DNAA's care — including members, volunteers, event participants, and service users.

3.4. Promote transparency, accountability, and trust in how DNAA handles data at all levels, from grassroots to governance.

4. Scope

4.1. This policy MUST be applied to all individuals processing DNAA data, including Executive Committee members, Officers, sub-committees, coaches, judges, event organisers, volunteers and any third-party processors acting on DNAA's behalf.

4.2. It covers all categories of DNAA data:

- **4.2.1.** Personal data
- **4.2.2.** Special-category data (e.g. medical details, DBS status, safeguarding records, data on minors)
- **4.2.3.** Archival records (minutes, governance files, historical documents)

4.3. It applies to all storage, transmission and processing media:

- **4.3.1.** Paper-based records
- **4.3.2.** Physical storage devices (USB drives, CDs, external hard disks)
- **4.3.3.** Electronic systems and services (local/network drives, personal devices, cloud platforms, email servers)
- **4.3.4.** SHOULD maintain an up-to-date register of all roles, systems and platforms used for DNAA data processing to ensure clear accountability and support audits.

5. Definitions

5.1. Personal Data

Any information relating to an identified or identifiable living individual (UK GDPR Art. 4(1)).

5.2. Special-Category Data

Personal data requiring extra protection under UK GDPR Art. 9, including health, disability, genetic/biometric data, trade-union membership, religious/philosophical beliefs, sex life/orientation, DBS status, safeguarding records or any data relating to minors.

5.3. Data Controller

The organisation or individual determining the purposes and means of processing personal data (UK GDPR Art. 4(7)).

5.4. Data Processor

A person or system that processes personal data on behalf of DNAA (UK GDPR Art. 4(8)).

5.5. Data Subject

The natural person whose personal data is being processed (UK GDPR Art. 4(1)).

5.6. Data Protection Lead

The individual appointed by DNAA to oversee data-protection compliance, handle subject-access requests, coordinate breach response, and act as liaison with the ICO.

5.7. Data Custodian

A DNAA-assigned individual responsible for the secure storage, access control, and retrieval of DNAA data.

5.8. Processing

Any operation performed on personal data, whether automated or not, including collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure, erasure or destruction (UK GDPR Art. 4(2)).

6. Roles & Responsibilities

6.1. Executive Committee MUST

6.1.1. Act as DNAA's Data Controller and ensure overall compliance with UK GDPR and the Data Protection Act 2018.

6.1.2. Appoint, support, and adequately resource the Data Protection Lead.

6.1.3. Approve this policy, associated procedures, and any major amendments.

6.1.4. Review significant data incidents, appeals, and any enforcement actions.

6.2. Data Protection Lead MUST

6.2.1. Oversee implementation of the Data Protection & Data Handling Policy.

6.2.2. Develop and deliver data-protection training, guidance and awareness sessions for all staff and volunteers.

6.2.3. Handle Subject Access Requests (SARs): verify identity, coordinate responses within 30 calendar days, and log each request in the Data-Subject Request Log (Appendix C).

6.2.4. Maintain records of processing activities (RoPA), Data Protection Impact Assessments (DPIAs), and the Breach Report Log (Appendix D).

6.2.5. Act as DNAA's primary liaison with the Information Commissioner's Office (ICO) and notify the ICO of any reportable personal-data breach within 72 hours.

6.3. Data Custodians SHOULD

6.3.1. Ensure accuracy, integrity, and appropriate accessibility of the data they hold.

6.3.2. Sign an annual Data Custodianship Agreement (Appendix B).

6.3.3. Keep an up-to-date inventory of DNAA data holdings and storage locations.

6.3.4. Apply suitable technical and organisational measures (encryption, secure backups, role-based access).

6.4. All Users MUST

6.4.1. Comply with every "MUST" clause in this policy.

6.4.2. Apply "SHOULD" guidance unless a documented, justified exception exists.

6.4.3. Complete mandatory data-protection training upon induction and refresher training annually.

6.4.4. Report any actual or suspected personal-data breach, loss, or unauthorised access immediately to the Data Protection Lead.

6.5. **Good Practice**- Publish an updated roles-and-responsibilities matrix after each AGM or officer change to maintain clarity and accountability.

7. Data Categories & Lawful Bases

7.1. Member Records

7.1.1. Examples: Name, address, date of birth, membership status

7.1.2. Lawful Basis (Art 6(1)(f) UK GDPR): Legitimate interests – necessary for administration of membership, event entry, communications

7.1.3. **Notes**: Document a Legitimate Interests Assessment (LIA) and publish a summary in your privacy notice

7.2. Special-Category Data

7.2.1. Examples: Health details, disability information, DBS status, safeguarding records, data on minors

7.2.2. Lawful Basis for processing (Art 6):
- Legal obligation (Art 6(1)(c)) – e.g. DBS checks, safeguarding requirements
- Explicit consent (Art 6(1)(a)) – where no legal obligation exists

7.2.3. Additional Condition (Art 9(2) UK GDPR): Must meet at least one condition, such as explicit consent (Art 9(2)(a)) or processing necessary for safeguarding (Art 9(2)(g))

7.3. Competition Results

7.3.1. Examples: Archer names, scores, event rankings

7.3.2. Lawful Basis (Art 6(1)(f) UK GDPR): Legitimate interests – transparent publication of results fosters fair competition and club promotion

7.3.3. Notes:
- Include a notice at event registration that results may be published.
- Allow entrants to object to publication where reasonable; document any opt-outs.

7.4. Archival Records

7.4.1. Examples: Meeting minutes, governance decisions, historical logs

7.4.2. Lawful Basis (Art 6(1)(c), (e) UK GDPR):
- Legal obligation – statutory record-keeping requirements
- Archiving in the public interest – long-term historical preservation

7.4.3. Retention: Indefinite, in line with your archival policy

7.5. Good Practice

7.5.1. Review all lawful-basis assignments and retention periods at least annually to reflect legal updates or operational changes.

7.5.2. Publish purpose-specific privacy notices where data is first collected, explaining your chosen lawful basis.

8. Data Lifecycle Management

8.1. Collection

8.1.1. MUST collect only personal data that is adequate, relevant and limited to what is necessary for the specified, explicit and legitimate purposes (UK GDPR Art 5(1)(c)).

8.1.2. MUST issue a privacy notice at or before the point of collection, setting out purposes, lawful basis, retention period and the Data Protection Lead's contact details (UK GDPR Arts 13–14).

8.1.3. SHOULD conduct a Data Protection Impact Assessment (DPIA) for any new or high-risk processing activities (UK GDPR Art 35).

8.2. Storage

8.2.1. MUST ensure personal and special-category data are protected by appropriate technical and organisational measures, including encryption at rest and in transit (UK GDPR Art 32).

8.2.2. SHOULD use DNAA-controlled systems with multi-factor authentication, regular backups and dual-access arrangements for critical records.

8.2.3. SHOULD test and review security measures periodically to confirm continued effectiveness (UK GDPR Art 32(1)(d)).

8.3. Access Control

8.3.1. MUST restrict access to personal data on a strict need-to-know basis, using role-based permissions (UK GDPR Art 5(1)(f)).

8.3.2. MUST review and update user access rights at least annually or whenever roles change.

8.3.3. SHOULD maintain an audit trail of data access and processing activities (UK GDPR Art 30).

8.4. Retention & Disposal

8.4.1. MUST retain personal and special-category data for no longer than necessary, in accordance with the retention periods documented in the Data Retention Schedule (Appendix A) (UK GDPR Art 5(1)(e)).

8.4.2. MUST retain archival records required by legal obligation or public-interest archiving, and document indefinite retention in the archival log (UK GDPR Arts 6(1)(c),(e)).

8.4.3. SHOULD review all retention schedules and disposal logs at least annually to confirm whether data can be securely destroyed.

8.4.4. MUST record every disposal action in the Disposal Log (Appendix A), including date, method, responsible person and witness (if applicable).

8.5. File Destruction Guidance

8.5.1. Physical File Destruction

8.5.1.1. MUST use an industry-standard cross-cut or micro-cut shredder (ISO/IEC 21964) for paper records.

8.5.1.2. MUST engage a licensed data-destruction service for bulk or highly sensitive archives and obtain a Certificate of Destruction.

8.5.1.3. MUST log all physical destruction activities in the Disposal Log (Appendix A).

8.6. Digital File Destruction

8.6.1. MUST use NCSC-approved secure-wipe utilities (e.g. Windows cipher /w, macOS Secure Empty Trash, Linux shred) for local drives and devices.

8.6.2. MUST apply ATA Secure Erase or full-disk overwrite for decommissioned hardware, following NCSC guidance.

8.6.3. SHOULD verify erasure effectiveness via recovery attempts or drive-health reports.

8.6.4. MUST record digital destruction details in the Disposal Log.

8.7. Cloud Storage & Backups

8.7.1. MUST permanently delete data—and all related backups/snapshots—in every region.

8.7.2. MUST revoke any access keys, credentials or service accounts associated with deleted data.

8.7.3. SHOULD obtain written confirmation of data purge from the provider.

8.7.4. MUST update the Cloud Inventory and Disposal Log with dates, methods and provider confirmations.

8.8. Good Practice: Maintain a central Retention Schedule and Disposal Log (Appendix A) to support regular audits.

9. Data Subject Rights & Requests

9.1. Rights Overview

9.1.1. Data subjects have the right to:

9.1.1.1. Access the personal data DNAA holds on them (UK GDPR Art 15).

9.1.1.2. Rectify inaccurate or incomplete data (Art 16).

9.1.1.3. Erase data where there is no overriding legal basis to retain it (Art 17).

9.1.1.4. Restrict processing in specified circumstances (Art 18).

9.1.1.5. Port data to another controller in a structured, commonly used format (Art 20).

9.1.1.6. Object to processing based on legitimate interests or direct marketing (Art 21).

9.1.1.7. Withdraw consent at any time where processing is based on consent (Art 7(3)).

9.2. Subject Access Requests (SARs)

9.2.1. Receipt & Logging

9.2.1.1. All SARs must be forwarded to the Data Protection Lead within 2 working days.

9.2.1.2. Log each request in the Data-Subject Request Log (Appendix C), assigning a unique Request ID.

9.3. Identity Verification

9.3.1. Verify the requester's identity before disclosing any data (UK GDPR Art 12(6)).

9.3.2. **Scope Determination**

- Confirm that the request concerns data held by DNAA only.
- Redirect Sport:80/membership-system enquiries to Archery GB.

9.4. Response Timeframe

9.4.1. Respond to valid SARs without undue delay and in any event within **1 calendar month** of receipt (Art 12(3)).

9.4.2. If the request is complex or numerous, you may extend by a further **2 months**, but you must inform the requester within the first month, explaining the reasons for delay.

9.5. Fees & Refusals

9.5.1. SARs are free of charge unless they are *manifestly unfounded* or *excessive*, in which case DNAA may charge a reasonable fee or refuse the request, documenting the rationale (Art 12(5)–(6)).

9.6. Format of Disclosure

9.6.1. Provide the data in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

9.6.2. Supply the information electronically in a structured, commonly used, machine-readable format unless the data subject requests otherwise (Art 20).

9.7. Refusal Notices & Appeals

9.7.1. If you refuse or partially refuse a request, issue a refusal notice within the statutory timeframe, stating the reasons, the right to complain to the ICO, and the right to seek a judicial remedy (Art 12(4)).

9.7.2. Any refusal or appeal may be escalated to the Executive Committee for review.

9.8. Good Practice

9.8.1. Use a standard SAR checklist (Appendix C2) to ensure all steps are followed.

9.8.2. Maintain templates for acknowledgment letters, data disclosures, and refusal notices to speed up responses.

10. Data Sharing & Third-Party Processors

10.1. Lawful Sharing

10.1.1. MUST only share personal data where DNAA has a valid lawful basis (UK GDPR Art 6) and, for special-category data, an Art 9 condition.

10.1.2. MUST share with Archery GB (via Sport:80) where necessary for membership verification, governance compliance, or safeguarding purposes, under lawful basis. Art 6(1)(b) (contract) and/or Art 6(1)(f) (**legitimate interests**).

10.1.3. MUST share with insurers, funders or legal authorities only where:

10.1.3.1. required by contract or legal obligation (Art 6(1)(b)/(c)); or

10.1.3.2. the data subject has given explicit consent (Art 6(1)(a) and, for special categories, Art 9(2)(a)).

10.2. Prohibited Disclosures

10.2.1. MUST NOT disclose personal data to commercial or other unauthorised parties.

10.2.2. MUST NOT use data for new purposes without updating privacy notices and confirming a lawful basis.

10.3. Data Processing Agreements

10.3.1. MUST have a written Data Processing Agreement (DPA) before any third party processes DNAA personal data (UK GDPR Art 28).

10.3.2. That DPA MUST:

10.3.2.1. specify subject-matter, duration, nature and purpose of processing;

10.3.2.2. set out security measures, confidentiality obligations and audit rights;

10.3.2.3. require the processor to assist DNAA with SARs, breach notifications and DPIAs;

10.3.2.4. ensure return or secure deletion of data at contract end.

10.4. International Transfers

10.4.1. MUST ensure any transfer outside the UK is lawful:

10.4.1.1. to a country with an Adequacy Decision; or

10.4.1.2. under Standard Contractual Clauses (SCCs) or another approved mechanism (UK GDPR Ch 5).

10.5. Documentation & Review

10.5.1. SHOULD maintain a register of all third-party data-sharing arrangements (Appendix F).

10.5.2. SHOULD review and re-sign DPAs at least every two years, or sooner if processing changes.

10.5.3. SHOULD conduct due-diligence and risk assessments (including DPIAs for high-risk processing) before onboarding any new processor.

10.6. ***Good Practice****:* Publish your Third-Party Register on the DNAA portal for transparency and audit readiness.

11. Role-Specific Expectations: Tournament Organisers & Bulk Communicators

11.1. Applicability

11.1.1. This section applies to any individual sending DNAA member or affiliate personal data to multiple recipients (e.g. event organisers, results coordinators, newsletter issuers).

11.2. Mandatory Requirements

11.2.1. All such communications MUST use the BCC (Blind Carbon Copy) field when including personal email addresses (UK GDPR Art 5(1)(f), Art 32).

11.2.2. The To and CC fields MUST only ever contain email addresses that are publicly available (for example, published DNAA committee contacts).

11.2.3. Any accidental exposure of personal email addresses (i.e. using To/CC in error) MUST be treated as a potential personal-data breach and reported under Section 12 (Incident Management & Breach Response).

11.3. Scope of Communications

11.3.1. Event invitations and logistical updates

11.3.2. Publication or circulation of competition results

11.3.3. Newsletters, surveys, and any other group correspondence involving DNAA data

11.4. Confidentiality Standard

11.4.1. Organisers MUST always adhere to DNAA's confidentiality principles, even where recipients are known to one another.

11.4.2. Where in doubt, default to BCC to safeguard member privacy.

11.5. Good Practice

11.5.1. Embed a default BCC reminder in all event-organiser and results-publishing email templates.

11.5.2. Include BCC etiquette in Tournament Organiser induction and refresher training materials.

12. Incident Management & Breach Response

12.1. Internal Reporting

12.1.1. MUST report all actual or suspected personal-data breaches to the Data Protection Lead as soon as possible and no later than 24 hours after discovery.

12.1.2. "Personal-data breach" includes any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

12.2. Breach Logging

12.2.1. 12.2.1 The Data Protection Lead MUST record each breach in the Breach Report Log (Appendix D), capturing at minimum:

12.2.1.1. Date/time discovered

12.2.1.2. Description and nature of the breach

12.2.1.3. Categories and approximate number of data subjects and records affected

12.2.1.4. Likely consequences for data subjects

12.2.1.5. Remedial and mitigation steps taken

12.2.2. If notification to the ICO is delayed beyond 72 hours, the reasons for delay MUST be documented here.

12.3. ICO Notification

12.3.1. Where a breach is likely to result in a risk to individuals' rights and freedoms, the Data Protection Lead MUST notify the ICO without undue delay and no later than 72 hours after becoming aware (UK GDPR Arts 33(1)–(2)).

12.3.2. The notification to the ICO MUST include:

12.3.2.1. Nature of the breach

12.3.2.2. Categories and approximate numbers of data subjects/records affected

12.3.2.3. Contact details of the Data Protection Lead

12.3.2.4. Likely consequences of the breach

12.3.2.5. Measures taken or proposed to address and mitigate the breach

12.4. Data Subject Notification

12.4.1. If the breach is likely to result in a high risk to data subjects' rights and freedoms, the Data Protection Lead SHOULD inform those individuals without undue delay (UK GDPR Art 34(1)).

12.4.2. Communications to data subjects SHOULD include:

12.4.2.1. Nature of the breach

12.4.2.2. Identity and contact details of the Data Protection Lead

12.4.2.3. Likely consequences

12.4.2.4. Measures taken or proposed to mitigate adverse effects

12.4.3. Where direct notification would involve disproportionate effort, a public statement or equivalent measure may be used instead.

12.5. Review & Testing

12.5.1. SHOULD conduct an annual tabletop exercise or simulated breach to validate response procedures and identify improvements.

12.5.2. After each real incident, the Data Protection Lead MUST lead a "lessons learned" review and update this policy or related processes as required.

12.6. ***Good Practice:*** Maintain an internal "near-miss" register of security incidents to proactively strengthen controls.

13. Contingency & Succession Planning

13.1. Custodianship Agreements

13.1.1. All Data Custodians MUST sign the annual Custodianship Agreement (Appendix B), confirming DNAA's ongoing ownership of the data and granting DNAA the right to access, duplicate or delete it at any time.

13.1.2. Each Agreement MUST record: data categories held, storage locations, backup schedules, and the identity of at least one secondary Exec-level custodian.

13.2. Shared Access & Backups

13.2.1. Critical DNAA data (membership records, governance documents, financials) MUST be stored in systems accessible by at least two named Executive Committee members, each with their own credentials.

13.2.2. Encryption keys, service-account credentials and device passwords SHOULD be held under dual-control in a secure custody arrangement.

13.2.3. Backups of all critical systems and data MUST be performed regularly, tested quarterly for restore capability, and retained in a geographically separate, secure location.

13.3. Inaccessibility Protocol

13.3.1. If a Data Custodian is unavailable, the Data Protection Lead or their deputy MUST attempt contact within 24 hours.

13.3.2. If contact cannot be made within 48 hours, the Data Protection Lead, with Executive Committee approval, MUST engage IT or service-provider support—using any lawful process necessary—to regain access.

13.3.3. All attempts, decisions and outcomes MUST be documented in the Breach & Incident Log (Appendix D) as a "continuity incident."

13.4. Exit & Handover Procedure

13.4.1. Departing staff or volunteers MUST:

13.4.1.1. Upon departure from role, the individual MUST transfer all DNAA data, system accounts, and credentials to a designated custodian or Executive Committee member, who will then initiate a password change or credential rotation for all affected platforms to ensure continued security and integrity.

13.4.1.2. Revoke and surrender any personal access rights (systems, devices, keys).

13.4.1.3. Securely delete any residual DNAA data on personal devices per Section 8.4 (Disposal Requirements).

13.4.2. The Data Protection Lead MUST verify completion of each step, record it in the Custodianship Register, and certify in writing that the handover is complete.

13.5. Good Practice

13.5.1. Following each AGM or major officer change, conduct a brief tabletop exercise to test access handover and continuity procedures.

13.5.2. Maintain a formal Business Continuity Plan that integrates data-recovery steps, role-succession details and contact lists for all key custodians.

14. Policy Review & Amendment

14.1. Review Frequency

14.1.1. MUST review this policy no less than once every 12 months.

14.1.2. MUST trigger an earlier review following any major incident, significant legal update, or substantial change in DNAA's processing activities.

14.2. Sources of Revision

14.2.1. SHOULD incorporate relevant findings from:

14.2.1.1. Breach reports, SAR logs, and near-miss registers

14.2.1.2. Volunteer feedback and training observations

14.2.1.3. Compliance audits or tabletop exercises

14.2.1.4. Changes to UK GDPR, Data Protection Act 2018, and ICO guidance

14.2.1.5. Updates in Archery GB policies or governance requirements

14.3. Approval & Communication

14.3.1. All amendments MUST be approved by the DNAA Executive Committee.

14.3.2. Changes MUST be communicated to all Officers, volunteers and Data Custodians within 30 days of approval.

14.3.3. SHOULD maintain a version-controlled changelog summarising revisions, dates and rationale.

15. Enforcement & Sanctions

15.1. Compliance Expectations

15.1.1. All individuals subject to this policy MUST comply with the “MUST” clauses in full.

15.1.2. “SHOULD” clauses represent recommended good practice and may be enforced where repeated or deliberate disregard causes risk to individuals, data integrity or DNAA's legal standing.

15.2. Internal DNAA Sanctions

15.2.1. DNAA may issue one or more of the following sanctions for breaches of this policy:

15.2.1.1. Verbal or written warnings

15.2.1.2. Mandatory retraining or re-induction

15.2.1.3. Suspension of role or access privileges

15.2.1.4. Removal from a voluntary role or office, in line with DNAA’s constitution and governance provisions

15.2.1.5. Referral to DNAA’s disciplinary process if applicable

15.3. Escalation Routes

15.3.1. Where a breach:

15.3.1.1. involves criminal activity (e.g. unauthorised disclosure, data theft, abuse),

15.3.1.2. poses a significant risk to data subjects, or

15.3.1.3. affects DNAA’s reputation or external compliance obligations,

15.3.2. DNAA MAY escalate the matter to:

15.3.2.1. **NCAS (Northern Counties Archery Society)** for regional governance review

15.3.2.2. **Archery GB** under their Code of Conduct, Safeguarding Policy or Disciplinary Regulations

15.3.2.3. **Information Commissioner’s Office (ICO)** if a serious breach of UK GDPR has occurred

15.3.2.4. **Local police or safeguarding authorities** where criminality, harm or child protection risks arise

15.3.3. The Data Protection Lead will assess severity in consultation with the Executive Committee and recommend escalation as appropriate. All such decisions MUST be documented in the Breach Report Log (Appendix D).

15.4. Remediation First

15.4.1. For minor breaches or process errors with limited impact, DNAA SHOULD offer remediation first—such as:

15.4.1.1. Retraining

15.4.1.2. corrective actions

15.4.1.3. monitored return to duties

—before formal sanctions are considered.

15.5. Fair Process

15.5.1. Any sanction or escalation MUST follow a fair and documented process, ensuring:

15.5.1.1. a clear account of the breach
15.5.1.2. an opportunity for the individual to respond
15.5.1.3. a proportionate decision based on risk, intent, and impact

15.6. ***Good Practice:*** DNAA should maintain a record of sanctions issued, anonymised for training and policy review purposes.

16. Data Retention

16.1. Retention Principles

16.1.1. DNAA MUST retain personal and special-category data only for as long as necessary to fulfil the specific purpose for which it was collected.

16.1.2. Indefinite retention is permitted ONLY for archival records, where justified under lawful bases defined in Section 7.

16.1.3. All retention periods MUST be documented in the Data Retention Schedule (Appendix A) and reviewed annually.

16.2. Scheduled Review & Disposal

16.2.1. Data Custodians MUST annually review the Retention Schedule and Disposal Log to identify records reaching end-of-life.

16.2.2. Expired data MUST be securely deleted or anonymised, in accordance with Section 9 (File Destruction Guidance).

16.2.3. Each disposal MUST be logged with:

16.2.3.1. Data category and description
16.2.3.2. Date and method of disposal
16.2.3.3. Responsible individual
16.2.3.4. Witness (if applicable)

16.2.4. SHOULD verify disposal through sample audits or system checks to confirm erasure effectiveness.

16.3. Archival & Historical Records

16.3.1. Records maintained for historical or governance purposes MAY be retained indefinitely if:

16.3.1.1. They meet a lawful basis under UK GDPR Art 6(1)(c) or 6(1)(e)
16.3.1.2. Their retention purpose is documented
16.3.1.3. They are stored securely and access is restricted
16.3.1.4. They are clearly separated from active personal records

16.3.2. Archival holdings SHOULD be reviewed periodically to ensure continued relevance and storage integrity.

16.4. Retention Following Role Changes

16.4.1. Upon role departure, the outgoing individual's data holdings MUST be assessed for relevance.

16.4.2. Non-essential records SHOULD be securely disposed of within 30 days.

16.4.3. The Data Protection Lead MUST confirm:

16.4.3.1. Retained data meets lawful basis criteria
16.4.3.2. Access permissions have been updated
16.4.3.3. Redundant records have been removed

16.4.4. 16.4.4 SHOULD conduct post-handover checks to prevent orphaned data and ensure continued data stewardship.

16.5. 16.5 Transparency & Privacy Notices

16.5.1. DNAA SHOULD inform data subjects of retention timelines during collection, via privacy notices or consent forms.

16.5.2. Any change to a published retention period MUST:

16.5.2.1. Be legally justified

16.5.2.2. Be documented in the Retention Schedule

16.5.2.3. Be communicated to affected individuals where feasible

INTENTIONALLY BLANK

Appendices

Appendix A – Data Retention Schedule (Template)

Data Category	Data Description	Lawful Basis	Retention Period	Data Owner / Custodian	Disposal Method	Next Review Date
Member Records	Registration forms, progression notes, attendance logs, membership payments	Contractual obligation (Art 6(1)(b))	7 years from last active membership	[Membership] Secretary / Treasurer / Chair	Secure shredding / encrypted deletion	xx/xx/xxxx
Special-Category Data	Medical disclosures, disability adjustments, safeguarding reports	Legal obligation (Art 6(1)(c)); special data (Art 9(2)(g))	7 years from case closure or last relevance	County Chair & DNAA Safeguarding Officer	Secure shredding / encrypted deletion	xx/xx/xxxx
Competition Results	Scores, ranking lists, classification updates, medal/trophy history	Legitimate interest (Art 6(1)(f))	Indefinite for published records; 7 years for raw data	DNAA Records Officer / Squad Manager	Secure deletion / archive migration	xx/xx/xxxx
Archival Records	Historical minutes, constitutional changes, precedent-setting governance decisions	Public task / legitimate interest (Art 6(1)(e)/(f))	Indefinite retention	DNAA Secretary	Review for historical value; otherwise shredding	xx/xx/xxxx
Correspondence Logs	Formal letters, decision notices, liaison with Archery GB or other bodies	Legal obligation / legitimate interest (Art 6(1)(c)/(f))	7 years from issuance	DNAA Secretary / County Chair	Secure shredding / encrypted deletion	xx/xx/xxxx
Volunteer Agreements	Role descriptions, welcome packs, consent forms, incident records	Contractual obligation / safeguarding (Art 6(1)(b)/(c))	7 years from last engagement	Safeguarding Officer	Secure shredding / encrypted deletion	xx/xx/xxxx
Coaching Records	Session logs, coach qualifications, mentoring notes	Legitimate interest / safeguarding (Art 6(1)(f)/(c))	7 years from last coaching engagement	DNAA Coaching Officer / Coaches / Safeguarding Officer	Secure shredding / encrypted deletion	xx/xx/xxxx

Incident & Accident Reports	Safety logs, equipment damage, near-miss records	Legal obligation / insurance (Art 6(1)(c))	7 years from report date or insurance settlement	Safeguarding Officer	Secure shredding / encrypted deletion	xx/xx/xxxx
Equipment Hire / Loan Records	Logs of club bows, arrows, and gear issued to members	Contractual obligation / legitimate interest (Art 6(1)(b)/(f))	3 years from return or resolution	Coaching Officer / Treasurer	Secure deletion / return logs archived	xx/xx/xxxx
Gift Certificates & Vouchers	Purchased or issued certificates and redemption history	Contractual obligation / financial records (Art 6(1)(b)/(c))	7 years from last transaction	Treasurer / [Membership] Secretary	Secure deletion / archived receipt logs	xx/xx/xxxx
Marketing & Consent Logs	Photo consents, social media permissions, newsletter opt-ins	Consent (Art 6(1)(a))	Until withdrawal or 2 years after last engagement	[Membership] Secretary / Treasurer / Chair	Secure deletion upon withdrawal	xx/xx/xxxx
Land & Lease Documentation	Field lease agreements, planning applications, council correspondence	Legal obligation / legitimate interest (Art 6(1)(c)/(f))	Indefinite or until lease termination	County Chair	Archive review and secure disposal	xx/xx/xxxx
Funding & Grant Applications	Applications, award letters, reporting documents	Public task / legitimate interest (Art 6(1)(e)/(f))	7 years from project close or grant audit	County Chair	Secure archive retention	xx/xx/xxxx
Digital Platform Logs	Discord onboarding flows, permissions, community moderation records	Legitimate interest / safeguarding (Art 6(1)(f)/(c))	2 years from onboarding or moderation action	Safeguarding Officer	Secure digital deletion / permission audits	xx/xx/xxxx
Supplier Communications	Uniform orders, equipment sourcing, service agreements	Contractual obligation / financial records (Art 6(1)(b)/(c))	7 years from transaction or dispute resolution	Treasurer	Secure email deletion / order archive	xx/xx/xxxx

Instructions:

- Complete each row with the appropriate details.

- Update the “Next Review Date” annually, if unsure, place AGM YYYY with the year it is due to be reviewed.
- When the retention period lapses, follow the disposal method and log completion.

Appendix B – Data Custodianship Agreement (Template)

*Please print your name in **BLOCK CAPITALS** and sign using **BLUE** ink.*

I, _____ (Full Name), in my capacity as _____ (Role), hereby acknowledge that I will hold and process data on behalf of Durham & Northumberland Archery Association (DNAA) in accordance with the DNAA Data Protection & Data Handling Policy Framework.

I confirm that:

- I have read and fully understood the DNAA policy.
- I accept and will adhere to all ***must*** requirements outlined therein.
- I will apply all ***should*** requirements as mandatory good practice, unless otherwise justified in writing.

I agree to the following conditions:

1. Data Accessibility & Control
   I will store DNAA data only using systems or locations that:
   - are approved by DNAA; and
   - allow access by at least two named members of the DNAA Executive Committee.
     If I am unable to meet this requirement, I will establish a contingency access arrangement—agreed in writing with DNAA—that ensures the organisation retains full, uninterrupted access to the data, including the right to retrieve, duplicate, or delete it as required. This agreement will be appended to this form.
2. Continuity of Custody
   I accept that DNAA data remains the property of DNAA at all times. I will ensure it remains:
   - Accurate and up to date
   - Stored securely
   - Accessible to DNAA in the event of my unavailability, incapacity, or departure
3. Exit & Withdrawal
   Upon leaving my role or at the formal request of DNAA, I will:
   - Transfer all DNAA data in my possession to the Executive Committee; and
   - Certify in writing that all copies have been securely deleted or destroyed from personal systems or devices
4. Ongoing Compliance
   I agree to participate in an annual review of this custodianship arrangement.
   I understand that failure to comply with this agreement, or with DNAA's Data Protection Policy, may result in formal disciplinary action.

Name (printed): _____
Signature: _____
Date: ____ / ____ / 20__
Role/Position: _____

Approved by (Data Protection Lead): _____
Signature: _____
Date: ____ / ____ / 20__

Appendix C – Data-Subject Request Log & SAR Checklist

C1. Data-Subject Request Log

Request ID	Requester Name	Date Received	Request Type (Access/Correction/Deletion)	Scope (DNAA / Sport:80 / Club)	Assigned To	Response Due	Outcome (Fulfilled/Refused/Redirected)	Date Closed	Notes
001									

Instructions:

- Assign a unique Request ID.
- Log every data-subject request, even if redirected.
- Update “Outcome” and “Date Closed” once complete.
- Use the SAR Checklist C2 for each request and ensure a copy is retained.

C2. SAR Checklist

Task	Status	Notes
Assign a unique Request ID		
Log every data-subject request, even if redirected		
Update “Outcome” and “Date Closed” once complete		
Verify requester’s identity (e.g. copy of photo ID)		
Determine scope of data held by DNAA; separate Sport:80 or club data		
Confirm lawful basis and any applicable exemptions		
Extract relevant records from all storage locations		
Review data for redaction (third-party information, sensitive notes)		
Draft response, attach privacy notice		
Send response within 30 days; record date and method		
Update Data-Subject Request Log		

Appendix D – Breach Report Log Template

Breach ID	Date/Time Discovered	Reported By	Description of Incident	Data Categories Affected	Immediate Actions Taken	Risk Level (High/Med/Low)	ICO Notified (Y/N)	Date Notified	Outcome / Remediation Measures	Closure Date
BR-001										

Instructions:

- Assign a unique Breach ID.
- Record full details as soon as a breach is suspected.
- Classify risk and note any regulatory notifications.
- Update “Outcome” and “Closure Date” when incident is resolved.
- Document lessons learned to improve future response.

Appendix E – Confidentiality Agreement (Template)

*Please print your name in **BLOCK CAPITALS** and sign using **BLUE** ink.*

This Confidentiality Agreement ("Agreement") is made on */*20__ between:

1. Durham & Northumberland Archery Association ("DNAA"), and
2. _____ ("Recipient"), in their capacity as _____.

3. Definitions
   - 3.1. "Confidential Information" means all non-public information disclosed by DNAA (in any form) to Recipient, including but not limited to:
     - 3.1.1. Personal Data and Special-Category Data (medical, DBS, safeguarding, financial, etc.) of members, volunteers, and competition entrants;
     - 3.1.2. Governance documents, minutes, policies, disciplinary records;
     - 3.1.3. Event details, entry lists, strategic plans, correspondence, and technical or commercial information.
   - 3.2. "Disclosing Party" means DNAA. "Receiving Party" means Recipient.
4. Obligations of Recipient
   - 4.1. Recipient **must** keep all Confidential Information strictly confidential and **must** not use or disclose it except as necessary to perform DNAA duties.
   - 4.2. Recipient **must** implement appropriate technical and organisational measures to protect Confidential Information from unauthorised access, loss, or disclosure.
   - 4.3. Recipient **must** not copy, reproduce, or transmit Confidential Information beyond what is strictly necessary, and all copies remain DNAA property.
   - 4.4. Recipient **must** disclose Confidential Information only to DNAA-authorised personnel on a strict need-to-know basis, provided those persons are bound by equivalent confidentiality obligations.
5. ExclusionsConfidential Information does **not** include information that:
   - 5.1. Is or becomes publicly available through no breach of this Agreement;
   - 5.2. Was rightfully known to Recipient prior to disclosure (with written proof);
   - 5.3. Is independently developed by Recipient without use of DNAA Confidential Information;
   - 5.4. Is lawfully obtained from a third party not under confidentiality obligation to DNAA.
6. Term & Duration
   - 6.1. This Agreement takes effect on the date above and continues:
   - 6.2. For as long as Recipient holds DNAA Confidential Information; and
   - 6.3. For 5 years thereafter (unless a longer period is required by law or policy).
   - 6.4. 4.2 Recipient's duty of confidentiality in respect of personal and special-category data continues for as long as DNAA is permitted to process such data under its Data Protection & Data Handling Policy.
7. Return & Destruction
   - 7.1. Upon request or termination of Recipient's role, Recipient **must** immediately return or securely destroy all Confidential Information (including electronic copies) and certify in writing that no copies remain.

8. Breach & Remedies
    8.1. Recipient acknowledges that any breach of this Agreement may cause irreparable harm to DNAA. DNAA **may** seek injunctive or other equitable relief, in addition to damages or any other remedy available at law.
9. Governing Law & JurisdictionThis Agreement **must** be governed by and construed in accordance with the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the English courts.

Signed for and on behalf of DNAA
Name: _____
Role: _____
Signature: _____
Date: /**/**20__

Signed by Recipient
Name: _____
Role/Position: _____
Signature: _____
Date: /**/**20__

Appendix F – Data Protection Template for use by clubs

This template is provided by DNAA to support local clubs in meeting their data protection responsibilities. It should be reviewed and adapted to reflect each club's size, structure, and operational context.

[Club Name] Data Protection & Handling Policy Template

Version: [Draft v1]
Release Date: [DD/MM/YYYY]
Review Date: [DD/MM/YYYY]

---

1. Policy Statement

[Club Name] is committed to full compliance with the UK GDPR and the Data Protection Act 2018. This policy sets out the mandatory requirements (MUST) and recommended practices (SHOULD) for the collection, storage, use, sharing, retention and disposal of personal and special-category data [1][2].

---

2. Scope

This policy applies to:

- This policy applies to all personal data processed by [Club Name], and to all personnel — including but not limited to officers, coaches, volunteers, event organisers, committee members and third-party processors acting on the club's behalf.
- All personal data and special-category data held by [Club Name], in any format (paper, electronic, audio, video).
- All systems and locations used to process data (local drives, cloud services, paper archives, mobile devices).

---

3. Definitions

Personal Data
Any information relating to an identified or identifiable living individual [UK GDPR Art 4(1)] [1].

Special-Category Data
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, health information, sex life or sexual orientation [UK GDPR Art 9] [1].

Data Controller
The organisation determining the purposes and means of processing personal data [UK GDPR Art 4(7)] [1].

Data Processor
An external party processing personal data on behalf of the Data Controller [UK GDPR Art 4(8)] [1].

Data Protection Lead
The individual appointed by [Club Name] to oversee data-protection compliance, handle data-subject requests and respond to breaches.

Processing
Any operation performed on personal data, including collection, recording, storage, use, disclosure, archiving or deletion [UK GDPR Art 4(2)] [1].

---

4. Roles & Responsibilities

Committee

- MUST appoint and support a Data Protection Lead.
- MUST inform DNAA Data Protection Lead of the Club Lead & Contact Details.
- MUST allocate sufficient resources for policy implementation, training and secure infrastructure.
- MUST review serious data incidents and approve remedial actions.

Data Protection Lead

- MUST maintain this policy, deliver training, handle Subject Access Requests (SARs) and lead breach investigations.
- MUST keep a log of all SARs, corrections, erasures and complaints.
- SHOULD conduct periodic audits of data processing activities.

All Staff & Volunteers

- MUST comply with every “MUST” requirement in this policy.
- SHOULD follow “SHOULD” guidance unless a documented justification exists.
- MUST report any actual or suspected data-protection breaches to the Data Protection Lead within 24 hours.

5. Data Categories & Lawful Bases

Data Category	Examples	Lawful Basis
Membership Records	Name, address, date of birth	Legitimate interests (Art 6(1)(f)) [1]
Special-Category	Health details, DBS checks	Explicit consent (Art 9(2)(a)) or legal obligation [1][2]
Competition Results	Scores, rankings, photographs	Legitimate interests for club purposes [1]
Communications Logs	Emails, letters, feedback	Legitimate interests (Art 6(1)(f)) [1]
Financial Records	Payment details, gift aid	Contractual necessity (Art 6(1)(b)) [1]

6. Data Lifecycle Management

Collection

- MUST only collect data necessary for specified purposes.
- MUST present a clear privacy notice at the point of collection [ICO Guidance].

Storage

- MUST store personal and special-category data in encrypted or physically secured locations.
- SHOULD use club-controlled platforms with role-based access controls.

Access Control

- MUST restrict data access to authorised roles on a need-to-know basis.

- SHOULD review user permissions immediately after any role change.

Retention & Disposal

- MUST retain personal and special-category data for no longer than seven years after membership expiry or last contact, unless a longer period is legally required [ICO Guidance].
- SHOULD maintain an up-to-date Retention Schedule (see Appendix A).
- MUST securely destroy paper records by cross-cut shredding and digital records using NCSC-approved wipe utilities.

---

7. Data Subject Rights & Requests

Data subjects are entitled to:

- Access their personal data (Subject Access Request).
- Rectify inaccurate or incomplete data.
- Erase data where no overriding legal obligation exists.
- Restrict or object to processing.
- Data portability where applicable (Art 15–22) [1].

Procedure

- MUST log every data-subject request in the Data Subject Request Log (Appendix B).
- MUST verify identity before responding.
- MUST respond to valid requests within 30 calendar days [ICO Guidance].
- SHOULD use the SAR Checklist (Appendix B) to ensure completeness.

---

8. Data Sharing & Third-Party Processors

- MUST only share data with Archery GB for membership verification, insurers, legal authorities or funders where contractually or legally required.
- MUST ensure any third-party processor signs a Data Processing Agreement reflecting UK GDPR obligations (Art 28) [1].
- SHOULD maintain a Third-Party Register and review processor compliance every two years.

---

9. Security & Breach Response

- MUST report any suspected personal-data breach to the Data Protection Lead within 24 hours.

- MUST record all breaches in the Breach Report Log (Appendix D).
- MUST notify the Information Commissioner's Office (ICO) within 72 hours if a breach risks individuals' rights or freedoms (Art 33–34) [1].
- SHOULD conduct an annual breach-response exercise.

---

10. Policy Review & Governance

This policy MUST be reviewed:

- Annually by the Committee.
- After any material change in processing activities or major data incident.

Amendments MUST be approved by the Committee and communicated to all staff and volunteers.

Appendices

- Appendix A: Retention Schedule Template
- Appendix B: Data Subject Request Log & SAR Checklist
- Appendix C: Breach Report Log Template
- Appendix D: Breach Report Log
- Appendix E: Roles & Contact Directory Template

(Placeholders in each Appendix should be completed by the Club before publication.)

References

[1] UK General Data Protection Regulation (EU) 2016/679 (as retained in UK law)
[2] Data Protection Act 2018
[3] Information Commissioner's Office guidance: "Personal data breaches: What to do and when to report"
[4] Information Commissioner's Office: "Data Sharing Code of Practice"

Appendix G – Section Summary/Quick Reference

1. Policy Statement

If you use DNAA data (names, health info, emails, scores, anything), you must protect it — legally, securely, and respectfully. This applies to everyone.

2. How to Use This Policy

“MUST” means legally required — no exceptions. “SHOULD” means recommended but can only be skipped with a documented reason. Stuck? Ask the Data Protection Lead or follow the strictest rule.

3. Purpose

This policy makes sure DNAA treats personal data properly, follows UK law, protects people’s rights, and builds trust.

4. Scope

Covers all data — personal, sensitive, historic — across paper, computers, phones, cloud, emails, and storage devices. If you handle DNAA data, this policy applies to you.

5. Definitions

Important legal terms are explained clearly so you know exactly what counts as “data,” a “processor,” or a “controller.” Use this if wording feels tricky or technical.

6. Roles & Responsibilities

Everyone has duties. Some roles (Execs, Protection Lead, Custodians) have extras like training others or handling breaches. Know your role and what’s expected of you.

7. Data Categories & Lawful Bases

Every bit of data needs a reason to exist. Depending on type, you’ll need consent, a legal duty, or a documented justification. What you collect, and why, must be clear and logged.

8. Data Lifecycle Management

From start to finish: collect only what’s needed, store it safely, give access only to the right people, and dispose of it securely when it’s no longer useful.

9. Data Subject Rights & Requests

People have rights over their data. They can ask to see it, fix mistakes, or request deletion. DNAA must respond clearly, fairly, and in a timely manner. Every request is logged.

10. Data Sharing & Third-Party Processors

Only share data with trusted partners if the law allows it. If someone outside DNAA handles data, there must be a written agreement, proper checks, and full records.

11. Role-Specific Expectations: Tournament Organisers & Bulk Communicators

If you send group emails or publish scores, use BCC. Never expose email addresses in public. If you slip up, it’s a breach — report it fast.

12. Incident Management & Breach Response

If data’s lost, exposed, or misused, it’s a breach. Report it within 24 hours, even if you’re unsure. DNAA follows a set process to fix issues and protect everyone involved.

13. Contingency & Succession Planning

No one should hold key data alone. Roles must have backups. Data access, storage, and handovers need clear plans — especially when someone leaves or is unavailable.

14. Policy Review & Amendment

This policy is checked every year or after big changes. Any updates must be agreed by DNAA’s Executive Committee and shared with everyone who uses or handles data.

15. Enforcement & Sanctions

Breaking this policy can lead to warnings, retraining, or removal from role. Serious breaches may be reported to Archery GB, the ICO, or police — depending on what happened.

16. Data Retention

DNAA only keeps data for as long as it’s needed. Once it's no longer useful or legally required, it must be securely deleted, anonymised, or archived. Every deletion is logged. Historical records can be kept permanently but must be stored safely and reviewed now and then.

If someone leaves a role, their data must be checked and cleared out if no longer relevant. Everyone should know how long their data is held, and if the timeline changes, DNAA has to explain why and update its records.