NATIONAL RIFLE ASSOCIATION

DATA PROTECTION AND DATA USE POLICY

Adopted by Council on 13 December 2025

NRA Data Protection and Data Use Policy

1. Policy Statement

The National Rifle Association (NRA) is committed to respecting and protecting the personal data of everyone we engage with. We recognise that individuals trust us with their information and expect us to handle it responsibly.

The NRA's objective is to comply fully with the UK General Data Protection Regulation (UK GDPR) and to be transparent in how personal data is used.

This policy sets out how the NRA complies with the UK GDPR, the Data Protection Act 2018, and the Data use and Access Act 2025 which strengthens requirements for transparency, ethical data reuse, and responsible data stewardship across the public and voluntary sectors.

2. Purpose of the policy

The purpose of this policy is to:

- Ensure we comply fully with relevant data protection laws and emerging legal responsibilities.
- Promote a culture of transparency, fairness, and accountability.
- Protect individuals' rights and freedoms regarding their personal data.
- Guide our approach to secure and ethical data sharing and reuse for public benefit.

3. Key Definitions

The NRA uses personal data, within the course of its business, for the administration and delivery of shooting competitions, training and membership services, as well as for personnel, administrative, financial, regulatory, payroll and organisational development purposes, including communication with members and stakeholders.

Article 4 of the UK GDPR defines the following key terms:

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Special Category Data: personal data of or regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data or health data.

Data Subject: An identified, or identifiable natural person.

Data Controller: The natural or legal person, public authority, agency, or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor: A natural or legal person, public authority, agency, or body which processes personal data on behalf of the controller.

Third Party: A body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Processing: An operation performed on personal data.

Pseudonymisation: Processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, otherwise processed.

Data Subject Consent: Means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

GDPR: refers to both the UK GDPR and, where applicable, the EU GDPR.

4. Policy Scope

This policy applies to:

- All employees, members, volunteers, trustees, consultants, contractors and agents acting on behalf of or representing the NRA ("associated persons").
- The storage and processing of personal data or sets of personal data in both electronic and paper formats, where the information is structured to allow access to details about individuals.
- All personal data processed by the NRA, regardless of where the individual is based. This includes data relating to members, donors, and other stakeholders within the UK and internationally.
- Any processing activities carried out by the NRA or its authorised third parties, whether the data is stored or accessed inside or outside the UK.

5. Procedures

5.1 The storage and processing of all personal data will be:

- Necessary for the NRA in delivering its charitable purposes and supporting beneficiaries, members and stakeholders;
- Retained only for the minimum period required to meet legitimate operational, legal, or regulatory requirements;
- Protected through appropriate internal and external security measures to ensure that only authorised personnel and approved third parties can access it;
- Deleted or anonymised upon request from the individual to whom the data relates, where the right to erasure applies under data protection law.

5.2 Justification for personal data

Personal data is processed in compliance with the six data privacy principles under Article 5 of the UK GDPR.

5.2.1 Personal data must be processed **lawfully, fairly,** and in a **transparent manner** in relation to the data subject.

5.2.2 Personal data can only be collected for specific, explicit, and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes.

5.2.3 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (**data minimisation**).

5.2.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

5.2.5 Personal data must be kept in a form such that the data subject can be identified only when necessary for processing; **(Storage limitation).**

5.2.6 Personal data must be processed in a manner that ensures the **appropriate security,** including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical measures.

The Controller must be able to demonstrate compliance with UK GDPR by maintaining clear policies, procedures, and plans in place to protect personal data and respond appropriately to any issues **(Accountability).**

5.3 Fair and lawful processing

We process personal data only where we have a lawful basis under GDPR. Depending on the purpose, this may include:

5.3.1 Consent – freely given, informed, and specific permission (e.g., to receive newsletters or to be photographed at events)
5.3.2 Contractual necessity – to fulfil agreements (e.g. processing memberships or event registrations)
5.3.3 Legal obligation – to comply with laws (e.g. safeguarding or financial reporting)
5.3.4 Vital interests – to protect someone's life (e.g. in medical emergencies)
5.3.5 Legitimate interests – for activities that individuals reasonably expect and which have minimal privacy impact (e.g. event planning, service improvement, managing memberships)

The NRA's Privacy Notice, available on our website, defines the legal basis for collecting personal data depending upon the data set.

5.4 Processing data in accordance with the individual's rights

The NRA will ensure that personal data collected, stored or processed is accurate, adequate, and relevant and not excessive. Personal data collected, stored or processed for one purpose will not

be used for any unconnected purpose unless the individual concerned has agreed to it or would otherwise reasonably expect it through legitimate interests.

To ensure transparency and where there is a legitimate basis for opting out, the data subject can decline the use of their personal data.

All staff who are responsible for collecting, storing or processing personal data are aware of the conditions for collecting, storing and processing personal data as laid out in this policy.

Under the UK GDPR, data subjects have the following rights:

5.4.1 **Right to be informed** – the right to be told how their personal data is used in clear and transparent language.
5.4.2 **Right of access** – the right to know and have access to the personal data we hold about them.
5.4.3 **Right to data portability** – the right to receive their data in a common and machine-readable electronic format.
5.4.4 **Right to be forgotten** – the right to have their personal data erased.
5.4.5 **Right to rectification** – the right to have their personal data corrected where it is inaccurate or incomplete.
5.4.6 **Right to object** – the right to complain and to object to processing.
5.4.7 **Right to purpose limitation** – the right to limit the extent of the processing of their personal data.
5.4.8 **Rights related to automated decision-making and profiling** – the right not to be subject to decision made without human involvement. We do not currently use automated profiling.

The NRA will comply with all valid requests, through a subject access request, unless there is a lawful exemption under the Data Protection Act 2018.

5.5 Procedure for making requests

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at dataprotectionofficer@nra.org.uk. The NRA will aim to provide the relevant data within one calendar month. If the request is complex or more than one request is made by an individual, the response time may be a maximum of three calendar months, starting from the day of receipt.[1]

[1] https://ico.org.uk/for-the-public/time-limits-for-responding-to-data-protection-rights-requests/

5.6 Disclosing data for other reasons

In certain circumstances, personal data may be disclosed to law enforcement agencies without the consent of the data subject where permitted by law. Under these circumstances, the NRA will disclose requested data. However, the NRA will ensure the request is legitimate, seeking assistance from legal advisers where necessary.

5.7 Data retention

Personal data shall be retained only for as long as necessary for the purpose for which it was collected. In some cases, data may be kept indefinitely for safeguarding, historical, archival, or legal purposes, where retention is justified and documented.

5.8 Sensitive personal data or "Special Category Data"

In almost all cases explicit permission from a data subject is required for storing, processing, or passing on Special Category Data unless, under exceptional circumstances, there is a safeguarding or legal requirement that overrides this regulation (Article 9 UK GDPR).

5.9 Privacy by design and default and Data Protection Impact Assessments (DPIAs)

The NRA adopts a privacy by design and default approach to all projects, systems, and processes that involve personal data. This ensures that data protection and privacy are considered from the earliest stages of any activity and throughout its lifecycle.

Under this approach, the NRA will:

5.9.1 Incorporate data protection and privacy safeguards into all new projects, systems and processes from the outset;

5.9.2 Ensure that only the minimum personal data necessary for each specific purpose is collected, processed and retained;

5.9.3 Apply the most privacy-friendly settings by default wherever possible, so that personal data is not accessible to unauthorised individuals or shared without a lawful basis; and

5.9.4 Review and update technical and organisational measures regularly to maintain compliance and protect individuals' rights.

Where processing is likely to result in a high risk to the rights and freedoms of individuals, the NRA will carry out a Data Protection Impact Assessment before the processing begins. The DPIA will:

(a) Describe the nature, scope, context, and purpose of the proposed processing;
(b) Assess the necessity and proportionality of the processing;
(c) Identify and evaluate risks to individuals; and
(d) Document the measures in place to mitigate those risks.

The Data Protection Officer is responsible for advising on and reviewing DPIAs, and must be consulted before any high-risk processing activity commences. Where a DPIA indicates that a high risk cannot be mitigated, the NRA will consult the Information Commissioner's Office (ICO) before proceeding.

All DPIAs will be retained as part of the NRA's data protection records and reviewed periodically to ensure ongoing compliance.

5.10 Reporting breaches

All suspected or confirmed data breaches must be reported immediately to the Data Protection Officer at dataprotectionofficer@nra.org.uk. The NRA will investigate promptly, contain the incident and assess risks to individuals. Data subjects affected or potentially affected will be informed as soon as possible after the NRA becomes aware of any breach.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the NRA will notify the (ICO) within 72 hours, as required by UK GDPR Article 33.

5.11 Training

All employees receive GDPR and IT training through an online training portal. Refresher training is scheduled annually.

6. Consequences of failing to comply with this Data Protection Policy

The NRA takes compliance with this policy very seriously. Failure to comply with this policy places members, employees, volunteers, trustees, contractors and other individuals as well as the organisation at risk and may lead to disciplinary or contractual action, up to and including dismissal or contract termination.

7. Monitoring and Review

This policy will be formally reviewed every three years. An interim review may be undertaken sooner where required due to legislative or regulatory changes, updated ICO guidance, or following any significant incident.

8. Resources and Publication

Related NRA policies:

(a) NRA Privacy Notice

(b) NRA Cookies Policy

(c) NRA Safeguarding Policy

(d) NRA Employee Handbook

The NRA will ensure that this policy is always publicly accessible on its website.

Version	Date created	Last review date	Next review date	Document Author
V1	13.12.2025	-	13.12.2028	Nicki Bahia