Approved: January 2026

Data Protection Policy

Purpose

This policy outlines how the Neurological Alliance of Scotland collects, uses, stores, and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Definition of personal data

“Personal data” means any information relating to an identified or identifiable living individual.

The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons.

If personal data can be truly anonymised then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.

Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

Information about companies or public authorities is not personal data.

However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

Scope

Applies to all trustees, consultants and volunteers who process personal data on behalf of the Neurological Alliance of Scotland.

Principles of data protection

The Neurological Alliance of Scotland will ensure that all personal data that it holds will be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
- adequate, relevant and limited to what is necessary (data minimisation)
- accurate and kept up to date (data accuracy)

- kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation)
- processed in a manner that ensures appropriate security of the personal data, including protection against accidental or unauthorised access to, or destruction, loss, use, modification, or disclosure of personal data (integrity and confidentiality).

We adhere to the following data protection principles:

1. **Personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject.**
   a) We provide clear information to individuals about what we are doing with their data.
   b) We are committed, when using legitimate interests, to balancing the rights of individuals, with regard to any vulnerability, against the interests of the Neurological Alliance of Scotland.

2. **Personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**.
   (a) We will not use the personal data for any other purpose unless this is compatible with our original purpose, we get consent, or we have a clear obligation or function set out in law.
   (b) Where we can process data further using our legitimate interests, we are committed to undertaking the balancing tests and being transparent about it.
   (c) If personal data is shared in any form, including anonymised personal data, we must ensure the individual has given full consent for the data to be used and is fully informed on how their data will be shared.

3. **Personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**
   (a) We will make sure that the personal data we are processing is:
      - adequate – sufficient to properly fulfil our stated purpose;
      - relevant – has a rational link to that purpose; and
      - limited to what is necessary – we do not hold more than we need for that purpose
   (b) We do not directly collect personal data from the general public and limit the collection of personal data from our members and trustees to that which is strictly necessary for the operation of NAoS.
   (c) Personal data collected from the general public in the My Neuro Survey is processed and stored by a third party fieldwork company and given to NAoS anonymised. We must adhere to the consent granted by the individual when completing the survey and ensure that any data collected is not being used outside of this remit.

4. **Personal data are accurate and, where necessary, kept up to date. Every reasonable step is taken to ensure that personal data are accurate, having regard to the purposes for which they are processed, are erased or rectified without delay**
   (a) Data subjects are informed of their rights to rectify data in our Privacy Policy.

(b) The Neurological Alliance of Scotland will take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact.

(c) We may need to keep the personal data updated, although this will depend on what we are using it for. The only personal data we regularly need to keep updated is that of our trustees outlined in our trustee register.

(d) If we discover that personal data is incorrect or misleading, we will take reasonable steps to correct or erase it as soon as possible.

5. **Personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.**

a) The Neurological Alliance of Scotland will not keep personal data for longer than we need it.

b) How long we keep personal data will depend on our purposes for holding the data. We have a separate record retention policy which outlines how long we keep personal data for and how it will be erased, anonymised, or removed from our systems

c) We may keep personal data for longer for public interest archiving, scientific or historical research, or for statistical purposes.

6. **Personal data are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

(a) The Neurological Alliance of Scotland takes the security of personal data extremely seriously. We do this in a variety of technical and organisational security measures, including but not limited to:

- We train our consultants, trustees and volunteers, where applicable, to handle data securely.
- our IT security policy covers technical measures such as passwords, two factor authentication, encryption, clarity on which systems must be used

(b) We have a cyber security policy for handling and reporting information security breaches, including reporting to the Information Commissioner's Office within 72 hours for significant breaches and notifying data subjects.

7. **The controller is responsible for, and should be able to demonstrate compliance with, the first six principles**

(a) We have created a framework of accountability (see below).

(b) We undertake data privacy impact assessments to mitigate the risk in line with all of the principles, and a record of these is kept.

(c) We keep records of our decisions.

8. **Accountability**

(a) Trustees have overall responsibility for ensuring compliance with GDPR legislation where relevant.

Approved: January 2026

Roles and Responsibilities

- The Board of Trustees is responsible for overall compliance.
- All consultants, trustees and volunteers must follow this policy when handling personal data.

Lawful Basis for Processing

We process personal data under the lawful bases of:

- Consent
- Contractual necessity
- Legal obligation
- Legitimate interests

Data Sharing and Third Parties

We do not sell or share data with third parties unless legally required or with explicit consent.

Data Security

- Digital data is stored securely with password protection and multifactor authentication.
- No paper files containing personal data will be held by trustees, consultants or volunteers except for in necessary circumstances. In the unlikely event paper files containing personal data are held by NAoS representatives, they should be kept securely in locked storage. Access is limited to authorised personnel.

Data Retention

- Personal data is retained only as long as necessary.
- Financial records are kept for 6 years in line with OSCR guidance.

Rights of Individuals

Individuals have the right to access their personal data and any such requests made to the Neurological Alliance of Scotland shall be dealt with in line with legal requirements, with some limited exceptions.

The UK GDPR provides the following rights for individuals in relation to their personal data:

- the right to be informed – we do this by making sure our privacy notices are correct and up to date and direct individuals to these notices on our website.
- the right to access their own data – any subject access requests must be notified to our Chair /Vice Chair who will co-ordinate a full search all of our systems before responding to the individual within 30 days, as required by law.

- rectification – we will quickly update any personal data which has been identified as inaccurate or incorrect.
- erasure – we will remove any personal data if an individual request this, unless we have another lawful bases which would prevent this.
- to restrict processing - where there is a dispute about the accuracy, validity or legality of personal data held by us, an individual has the right to require us to cease processing the data for a reasonable period of time to allow the dispute to be resolved.
- the right to data portability - we will provide an individual with their data in a common and machine-readable electronic format.
- the right to object – complaints or objections to processing personal data will be dealt with quickly and accurately.
- rights in relation to automated decision making and profiling – we do not carry out any automated decision making or profiling of any individual.

Data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All trustees, consultants and volunteers must be able to identify a suspected personal data breach.

A breach could include:

- access by an unauthorised third party to personal data;
- deliberate or accidental action (or inaction);
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data;
- leaving a file on a train.

Where a trustee, consultant or volunteer discovers or suspects a personal data breach, this should be reported to the chair of the board as soon as possible.

Where there is a likely risk to individuals' rights and freedoms, the chair of the board will report the personal data breach to the ICO within 72 hours of the Neurological Alliance of Scotland being aware of the breach. Should the chair be unavailable reporting to the ICO will be the responsibility of the Vice Chair or nominated trustee.

Where there is also a likely high risk to individuals' rights and freedoms, we will inform those individuals without undue delay.

Approved: January 2026

The chair of the board will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

Privacy by design

Privacy by design is an approach that promotes privacy and data protection compliance from the beginning.

Trustees, consultants and volunteers must become familiar with this policy and include privacy and good data protection practices as core within any new project design or any material change to an existing project/work.

If you have any questions, concerns or need help or advice about any aspect of Data Protection, contact our chair of the board.