BrainWaves Research Data Protection Policy

1. Introduction and Scope

This policy outlines BrainWaves Research's commitment to data protection and its compliance with UK data protection legislation, specifically the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

The purpose of this policy is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of BrainWaves Research, including trustees, staff, and volunteers.

2. Data Protection Lead

BrainWaves Research has appointed a Data Protection Lead who is responsible for overseeing data protection compliance and leading on any incident investigation and reporting. The Data Protection Lead is Natalie Coles and can be contacted at **data.protection@brainwaveshub.org**.

The Data Protection Lead will also ensure that all staff and volunteers are provided with induction, on-the-job, or other necessary training and are made aware of their data protection responsibilities.

3. Key Definitions

- **UK GDPR:** The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.
- **Data Processor:** An individual or organisation that processes personal data on behalf of a data controller.
- **Data Controller:** An individual or organisation that determines how and why personal data is processed. BrainWaves Research is the Data Controller for the personal data it holds.
- **Data Subject:** An individual whose personal data is being processed.
- **Processing:** Any operation performed on personal data, including collection, storage, use, and disclosure.
- **Personal Data:** Any information that can identify a living individual, such as name, address, or email address.
- **Sensitive Personal Data (or 'Special Category Data'):** Personal data that requires extra protection, such as information on health, ethnic origin, religious beliefs, or sexual orientation.
- **Direct Marketing:** Any communication aimed at promoting a product or service directly to an individual.
- **PECR:** The Privacy and Electronic Communications Regulations, which govern electronic direct marketing and the use of cookies.

- **Valid Consent:** Consent that is freely given, specific, informed, and an unambiguous indication of the data subject's wishes. It can be withdrawn at any time.
- **Legal Basis for Processing:** A lawful reason for processing personal data, which includes consent, contract, legal obligation, vital interests, public task, and legitimate interests.

4. Data Protection Principles

We will adhere to the data protection principles, ensuring that data is:

- **4.1. Processed lawfully, fairly, and in a transparent manner.**
    - We will have a valid legal basis for all data processing activities, which may include obtaining explicit consent from individuals, fulfilling a contractual obligation, or pursuing a legitimate interest of the charity.
    - We will be open and honest about how and why we collect data. Individuals have the right to access their data.
- **4.2. Collected for specified, explicit, and legitimate purposes and not used for any other purpose.**
    - We are clear on what data we will collect and the specific purpose for which it will be used.
    - We will only collect data that is necessary for the stated purpose.
    - Data will not be used for any other purpose without the data subject's consent or another valid legal basis.
- **4.3. Adequate, relevant, and limited to what is necessary.**
    - We will ensure that all personal data collected is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. We will not collect or hold excessive data.
- **4.4. Accurate and, where necessary, kept up to date.**
    - We will take reasonable steps to ensure that the data we hold is accurate and up-to-date.
    - We will have processes and/or checks to ensure that data which needs to be kept up-to-date is.
    - We will promptly correct any inaccuracies identified.
- **4.5. Kept for no longer than is necessary.**
    - We will only hold personal data for as long as required to fulfil the purpose for which it was collected, or to meet a legal or administrative requirement.
    - We will maintain a Data Retention Schedule outlining retention periods for different categories of data, which will be available upon request.
    - Both hard copy and electronic data will be securely disposed of or destroyed when no longer needed.
- **4.6. Processed to ensure appropriate security, including protection against unlawful use, loss, or damage.**
    - Data is held securely and access is restricted to those who need it.

- Paper documents are locked away. Access to online folders is restricted. IT systems are password-protected, and sensitive documents are password-protected.
- Our IT systems will have adequate and up-to-date anti-virus and firewall protection.
- Staff and volunteers will be trained on safeguarding against cyber-attacks, and on the importance of using strong, unique passwords that are never written down or shared.
- We have adequate data backup and disaster recovery processes in place to ensure data is recoverable in the event of a system failure or data loss.

5. Individual Rights

We recognise and will respect the rights of individuals concerning their personal data under the UK GDPR. These rights include:

- The right to be informed.
- The right of access.
- The right to rectification (correction of inaccurate data).
- The right to erasure (the 'right to be forgotten').
- The right to restrict processing.
- The right to data portability.
- The right to object to processing.
- The right in relation to automated decision-making and profiling.

6. Use of Imagery/Video

All imagery is protected by copyright. Additionally, the use of images and videos of individuals or small groups falls under data protection law. We will:

- Obtain explicit consent from individuals before using their images, particularly when the image is of an individual or small group.
- Exercise particular care when using images of children or other vulnerable people, and ensure valid consent from a parent or guardian is obtained where necessary.
- Ensure that individuals are informed of the specific purpose for which their image will be used.
- Provide a chance for individuals to opt out of photographs in large groups.
- Take care not to use images of children or vulnerable people in a way that could place them at risk, especially on public platforms.

7. Data Breach

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

In the event of a data breach, we will immediately investigate the circumstances to identify what action needs to be taken.

We will notify the ICO within 72 hours of a breach if it is likely to result in a significant risk to the rights and freedoms of individuals. This includes breaches that could lead to discrimination, damage to reputation, financial loss, or loss of confidentiality.

8. Fundraising

We will ensure that our fundraising complies with the UK GDPR and ICO guidelines, as well as the **Fundraising Regulator's Code of Fundraising Practice**. We will respect the privacy and contact preferences of our donors.

We will respond promptly to requests to cease contact or to complaints, and will take action to address their causes.

9. Artificial Intelligence

We have adopted and comply with the ICO AI guidance. We recognise the importance of human oversight, and will ensure all AI-assisted decisions are reviewed by a human and that any personal data used in AI systems is processed in compliance with the principles outlined in this policy.

10. Data Retention

Our data will only be kept for as long as there is a legal, administrative, or operational need to do so. We maintain a detailed Data Retention Schedule that specifies how long different types of records are kept.

In general, records are kept for a minimum of 6 years after the end of the accounting year to which they relate to meet legal requirements, but we do not keep personal records any longer than necessary. Factors affecting retention periods include legal requirements, storage costs, historical value, and archival needs.

BrainWaves Research

Date Adopted: 28 August 2025

Date of Next Review: October 2025 (and annually thereafter)