



HOPE Charity Project - Data Protection Policy (UK-GDPR)

Last Reviewed: 07 July 2025

Review Date: 07 July 2026

Version: 2.0

1. Overview of Data Protection at HOPE

HOPE Charity Project is committed to protecting the personal information of the young people, families, staff, volunteers, and supporters we work with. We only collect data that is necessary, relevant, and proportionate, and we store it securely using OneDrive and other secure systems.

This policy explains how we comply with the United Kingdom General Data Protection Regulation (UK-GDPR) and what steps we take to protect people's information. It reflects our commitment to confidentiality, transparency, and respectful practice - especially in the context of early intervention and emotional wellbeing.

2. Contact and Responsibility

Claire Sparrow, Founder and Lead, is responsible for overseeing data protection within the charity. She can be contacted at:

Name: Claire Sparrow

Role: Founder and Lead

Email: Claire@hopecharityproject.org

Address: HOPE Charity Project, Wild Heart Hill, Findon, West Sussex

Phone: 07789154690

3. Our Commitment to UK-GDPR Principles

HOPE Charity Project ensures that all personal data we handle is:

- Processed lawfully, fairly, and transparently
- Collected for clear, legitimate purposes and not used in unrelated ways
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date where needed
- Stored only as long as necessary
- Protected by appropriate security measures (both technical and organisational)

4. Lawful Basis for Processing Data

Under UK-GDPR, we must have a lawful basis for collecting and using personal data. At HOPE Charity Project, we rely on the following:

4.1 Consent – We collect contact information from families, volunteers, and supporters who give us clear permission to get in touch.

4.2 Contract – We collect information to manage agreements with service providers.

4.3 Legal Obligation – We collect data when legally required to do so, such as financial or safeguarding records.

4.4 Legitimate Interest – We use data to operate smoothly and offer appropriate support, always with a focus on privacy and respect.

5. Individual Rights

Everyone whose data we hold has the right to:

- Be informed
- Request access
- Ask us to correct errors
- Withdraw consent
- Request deletion
- Raise concerns with the ICO

6. Scope and Sensitivity of Data

We hold basic personal information on families, volunteers, professionals, and donors. This includes:

- Names and contact details
- Notes on services received (non-clinical)
- Referral or attendance information

We store data securely on OneDrive with access controls.

7. Who Is Responsible?

HOPE Charity Project is a registered data controller under the UK General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018. We are responsible for the personal information we hold and process.

We do not appoint a formal Data Protection Officer. Instead:

- Claire Sparrow leads data protection.
- Only authorised team members access data.
- Volunteers and staff receive basic data protection training.
- Third-party tools like OneDrive are used with care and GDPR compliance checks.

8. How We Collect and Store Personal Data

We collect data via:

- Referral or welcome forms
- Conversations
- Volunteer/supporter sign-up forms
- Supplier records

Stored securely on OneDrive, with access restricted to relevant team members.

9. Data Retention

- Service user data: 6 years after last contact
- Volunteer/staff contact: deleted after 6 years of stepping down
- Supporters: kept while consent remains valid
- Financial data: 6 years for HMRC

Reviewed annually and securely deleted when no longer needed.

10. Third Party Access

We never sell or share personal data for marketing. We only share when:

- Required by law
- Necessary for services
- Tools (like OneDrive) are used securely

11. Data Breaches

Any breach is:

1. Assessed and contained
2. Reported to ICO within 72 hours (if required)
3. Communicated to affected individuals
4. Logged and reviewed

12. Data Protection Impact Assessment (DPIA)

We review data use regularly to check:

- What we hold
- Where it's stored
- Risks and areas to improve

We seek advice when needed, especially before changes.

13. Privacy Notices

We always inform people about what data we're collecting, why, and how it will be used. Privacy Notices are provided when data is collected directly, or at the earliest opportunity if collected indirectly.

14. Contact for Data Questions or Concerns

Anyone with concerns or questions about their data can contact:

Claire Sparrow

Founder and Lead

Claire@hopecharityproject.org

15. Updates to This Policy

This policy is reviewed yearly or sooner if needed. Latest version stored in internal files and shared with funders or partners on request.

Data Retention Summary – HOPE Charity Project

To comply with UK GDPR and safeguard best practice, HOPE Charity Project retains personal data only for as long as necessary. The following retention periods apply:

Support Service Records

- Case notes, visitor logs, support plans: Retained for 6 years from the last contact date.
- If the record involves a child or young person, retain until the individual turns 25.

Safeguarding Records

- General concerns or referrals: Retain for 6 years
- Serious incidents or formal investigations: May be kept indefinitely if necessary to protect others or if advised by authorities.

Volunteer and Staff Records

- Personnel files, references, training records: Retained for 6 years after departure
- DBS check outcomes (date and number only): Retained for duration of role plus 6 months after leaving

General Correspondence and Enquiries

- Emails, phone logs, and informal queries: Retain for up to 2 years, unless they relate to ongoing support or safeguarding.
- These are reviewed annually and deleted when no longer needed.

Financial Records

- Invoices, donations, expense claims, payroll (if applicable): Retained for 6 years to meet HMRC and Charity Commission requirements

All records are stored securely on OneDrive with access limited to authorised team members. When retention periods end, data is permanently deleted or anonymised unless required for ongoing safeguarding or legal reasons.