Hummingbird Community Activities

Data Protection & Confidentiality Policy

Owner: Joanna Kusnierek
Organisation: Hummingbird Community Activities
Version: 1.0
Date: June 2026

1. Policy Statement

Hummingbird Community Activities is committed to protecting the privacy, dignity, and rights of all individuals who use our services, including adults and children with additional needs.

We recognise that we hold sensitive personal information and we will ensure it is:

- Collected fairly and lawfully
- Used only for legitimate purposes
- Kept secure and confidential
- Shared only when necessary and appropriate

We comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant safeguarding legislation.

2. Scope

This policy applies to:

- All staff (paid or voluntary)
- The owner and management
- Contractors or external professionals
- Anyone handling personal data on behalf of the organisation

3. Types of Data We Collect

We may collect and store the following information:

Personal Data

- Name, address, date of birth

- Emergency contact details
- Attendance records

Sensitive (Special Category) Data

- Medical conditions and disabilities
- Care plans and support needs
- Medication details
- Behavioural information
- Safeguarding concerns
- Disability-related risk assessments

4. Lawful Basis for Processing Data

We process personal data under the following lawful bases:

- **Consent** (where appropriate, e.g. photographs or newsletters)
- **Vital interests** (emergency situations)
- **Legitimate interests** (service delivery and administration)
- **Legal obligation** (safeguarding and reporting requirements)
- **Special category data** is processed for health, care, and safeguarding purposes

5. Principles of Data Protection

We follow these key principles:

- Data is used fairly, lawfully, and transparently
- Only necessary data is collected
- Data is kept accurate and up to date
- Data is not kept longer than needed
- Data is stored securely
- Individuals' rights are respected

6. Confidentiality

All personal information is treated as strictly confidential.

Staff must:

- Only access information needed for their role
- Not discuss service users outside of professional need
- Never share personal details on social media
- Ensure conversations about service users are private

Confidentiality may be broken only when:

- There is a safeguarding concern
- A person is at risk of harm
- Required by law or statutory authority

7. Data Storage and Security

We ensure data is protected through:

Physical Records

- Stored in locked cabinets
- Access restricted to authorised personnel only

Digital Records

- Password-protected systems
- Secure devices only
- No personal data stored on unsecured personal devices

Communication

- Sensitive information is not sent via unsecured email or messaging services unless encrypted or approved

8. Data Retention

We only keep data for as long as necessary.

Typical retention periods:

- Service user records: up to 6 years after service ends (or longer if required for safeguarding/legal reasons)
- Accident and incident records: minimum 6 years
- Safeguarding records: retained in line with safeguarding guidance

After retention periods, data will be securely destroyed.

9. Data Sharing

We may share information only when necessary and appropriate with:

- Family members or carers (with consent where possible)
- Social services
- Health professionals (GPs, nurses, therapists)
- Local authority safeguarding teams
- Emergency services

We will:

- Share only relevant information
- Record what has been shared and why
- Ensure secure transfer methods

10. Individual Rights

Service users (or their representatives) have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request deletion (where legally possible)
- Restrict or object to processing
- Withdraw consent (where applicable)

Requests should be directed to the organisation owner.

11. Data Breaches

A data breach includes accidental or unlawful loss, disclosure, or access to personal data.

In the event of a breach:

1. It will be reported immediately to the owner (Joanna Kusnierek)
2. The risk will be assessed
3. Steps will be taken to contain and prevent further breach
4. If necessary, the Information Commissioner's Office (ICO) will be notified within 72 hours
5. Affected individuals will be informed where required

12. Safeguarding and Confidentiality Balance

Where confidentiality conflicts with safeguarding, the safety and wellbeing of the individual takes priority.

Information may be shared without consent if:

- A child or vulnerable adult is at risk
- There is risk of serious harm
- Required by safeguarding law or procedure

13. Staff Responsibilities

All staff must:

- Follow this policy at all times
- Complete required data protection training
- Report concerns or breaches immediately
- Ensure secure handling of all information

14. Policy Review

This policy will be reviewed:

- Annually, or
- When legislation changes, or
- When organisational practice changes

15. Contact Information

Data Controller: Joanna Kusnierek
Organisation: Hummingbird Community Activities