Data Protection Policy

Widecombe Community Hall CIO

Date Approved: 23rd March 2026

Review Date: March 2027

1. Introduction and Scope

This policy outlines Widecombe Community Hall's commitment to data protection and compliance with the UK Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). 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 Widecombe Community Hall CIO, including trustees, volunteers, and any contractors or partners.

As a small community hall charity, the personal data we hold is limited but still important. It typically includes contact details of hall hirers and regular users, trustee and volunteer records, event photography, and financial records relating to bookings and payments.

2. Data Protection Lead

The charity will appoint a Data Protection Lead from among the trustees. The Data Protection Lead will be responsible for:

- Overseeing compliance with this policy and data protection law.
- Leading on the investigation and reporting of any data breach.
- Ensuring that all trustees and volunteers receive appropriate guidance on their data protection responsibilities as part of their induction.
- Acting as the first point of contact for any data protection queries or concerns.

The name and contact details of the Data Protection Lead will be displayed in the hall and on the charity's website or noticeboard.

3. Key Definitions

UK GDPR: The UK General Data Protection Regulation, which sets out the rules for processing personal data in the UK.

Personal Data: Any information that can identify a living individual, such as name, address, email address, or telephone number.

Special Category Data: Personal data that requires extra protection, such as information about health, ethnic origin, religious beliefs, or sexual orientation.

Data Controller: The organisation that decides how and why personal data is processed. For the purposes of this policy, this is Widecombe Community Hall.

Data Processor: Any individual or organisation that processes personal data on our behalf.

Data Subject: An individual whose personal data is being processed.

Processing: Any operation performed on personal data, including collection, storage, use, disclosure, and deletion.

Valid Consent: Consent that is given freely, for a specific purpose, fully informed, and which can be withdrawn at any time.

4. Data Protection Principles

We will ensure that all personal data is:

- **Processed lawfully, fairly and transparently.** We will be open and honest about what data we collect and why. Where consent is the basis for processing, we will obtain clear consent and respect individuals' right to access their data.
- **Collected for specified, explicit and legitimate purposes.** Data collected for one purpose will not be used for another without the consent of the individual concerned.
- **Adequate, relevant and limited to what is necessary.** We will only collect the data we need and no more.
- **Accurate and kept up to date.** We will take reasonable steps to ensure personal data is accurate and correct any errors promptly.
- **Kept for no longer than necessary.** We will retain data only for as long as there is a legitimate need, in accordance with our data retention schedule (see Section 10). This applies to both paper and electronic records.
- **Processed securely.** We will follow ICO guidance on data storage, sharing, and security. Data will be held securely so that it can only be accessed by those who need to, whether in paper form (locked away) or electronic form (password-protected). We will maintain adequate protections against cyber threats and ensure data can be recovered in the event of loss.

5. Individual Rights

Under the UK GDPR, individuals have a number of rights in relation to their personal data. We recognise and will respect the following rights:

- The right to be informed about how their data is used.
- The right to access their personal data.
- The right to rectification 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.

Any individual wishing to exercise these rights should contact the Data Protection Lead. We will respond to any valid request within one calendar month.

6. Use of Imagery and Video

Photographs and videos taken at hall events may contain personal data and must be handled with care. The following principles apply:

- Images taken for one purpose (such as personal use) must not be used for another (such as publicity) without consent.
- For photographs of individuals or small groups, an image consent form should be used.
- When photographing large groups at events, individuals should be given a reasonable opportunity to opt out.
- Particular care must be taken with images of children or vulnerable people. Valid consent must be obtained, and we must be confident that publication will not place anyone at risk.
- Anyone featured in an image should be told how it will be used, and the image must only be used in accordance with what they were told.

7. Children and People Who Lack Capacity

The community hall hosts events and activities that may involve children and people who may lack the capacity to give informed consent. The following provisions apply:

- Children under 13 cannot legally give consent for the processing of their personal data. Consent must be obtained from a parent or guardian.

- Privacy notices or information provided to children should be written in clear, age-appropriate language.
- Where an individual lacks the capacity to give consent, consent must be obtained from the person legally authorised to act on their behalf, such as someone with a Lasting Power of Attorney.
- Any decisions made regarding the personal data of people who lack capacity must be made in their best interests.

8. Data Breach

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes not only loss of data but also unauthorised access or sharing.

In the event of a suspected breach, the Data Protection Lead will:

- Investigate the circumstances promptly to establish the facts.
- Take immediate steps to contain the breach and limit any damage.
- Assess whether the breach is likely to result in a risk to the rights and freedoms of any individuals affected.
- If so, notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.
- Inform affected individuals without undue delay where there is a high risk to their rights and freedoms.
- Record the breach and the charity's response, regardless of whether it was reported to the ICO.

Examples of breaches that are likely to require reporting include those that could result in discrimination, reputational damage, financial loss, or loss of confidentiality.

Following any breach, the trustees will review procedures and take steps to prevent recurrence, including disciplinary action where appropriate.

9. Data Protection Complaints

In line with ICO guidance and the Data (Use and Access) Act 2025, anyone who believes we have not handled their personal information appropriately may raise a data protection complaint.

We will:

- Provide a clear and accessible way for individuals to submit data protection complaints, via the Data Protection Lead.
- Acknowledge receipt of any complaint within 30 calendar days.
- Investigate the complaint without undue delay, keeping the complainant informed throughout.
- Communicate the outcome promptly and clearly, explaining any actions taken or decisions made.

All complaints will be handled fairly, transparently, and in accordance with our obligations under the Data Protection Act. If the complainant remains dissatisfied, they may escalate the matter to the Information Commissioner's Office (ICO).

10. Data Retention

Personal data will only be kept for as long as there is a legitimate administrative need, or for as long as required to meet legal or audit obligations.

As a general guide:

- Financial and accounting records: 6 years after the end of the accounting year to which they relate, as required by HMRC.

- Trustee and volunteer records: for the duration of their involvement, plus a reasonable period thereafter.
- Hall booking records and hirer details: for the current year plus the previous year, unless a longer period is needed for insurance or dispute resolution purposes.
- Event photographs: reviewed annually and deleted when no longer required.

The Data Protection Lead will carry out an annual review to ensure that personal data no longer needed is securely deleted or destroyed, covering both electronic and paper records.

11. Related Policies

This policy should be read alongside the charity's other relevant policies, including:

- Equality, Diversity and Inclusion Policy
- Safeguarding Policy (if applicable)
- Complaints Policy
- Health and Safety Policy

12. Help and Support

The Information Commissioner's Office (ICO) provides guidance and resources for charities on data protection compliance. Further information, including a self-assessment tool for small organisations, is available on the ICO website at ico.org.uk.

Version Control – Approval and Review

Version	Approved By	Approval Date	Main Changes	Review
1.0	Board	Oct 2023	Initial draft approved	Annually
1.1	Board	Jun 2024	Retention periods added	Annually
2.0	Board	Mar 2026	Full review: added complaints procedure, practical data inventory guidance, imagery consent, children and vulnerable persons provisions, breach response procedure	Annually

Acknowledgement

This policy was developed with reference to the template provided by Charity Excellence Framework (charityexcellence.co.uk).