



# Data Protection Policy & Procedures

## 1. Introduction

---

Offord Village Hall ("the Charity") is committed to protecting the rights and privacy of individuals. We collect and use certain personal information in order to manage the hall, its hirings, finances, fundraising, and community activities. This personal information must be collected, handled, stored, and disposed of in compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

This policy applies to all trustees, volunteers, contractors, and anyone handling personal information on behalf of the Charity.

## 2. Key Roles

---

- **Data Controller:** The trustees of Offord Village Hall, who decide what data is collected, how it is used, and for what purposes.
- **Data Protection Lead:** A named trustee will act as the point of contact for data protection matters. (Name to be inserted once appointed.)
- **Information Commissioner's Office (ICO):** The UK regulator responsible for enforcing data protection law.

## 3. Principles of Data Protection

---

We will comply with the **7 key principles of UK GDPR**. Personal data must be:

1. **Lawful, fair and transparent** – processed fairly, lawfully and openly.
2. **Purpose limited** – collected for specified purposes only.
3. **Data minimised** – adequate, relevant, and limited to what is necessary.
4. **Accurate** – kept accurate and up to date.
5. **Storage limited** – kept only as long as necessary.

6. **Secure** – processed securely, with protection against unauthorised access, loss or damage.
7. **Accountable** – we must be able to demonstrate compliance with all principles.

#### 4. Lawful Bases for Processing

---

We will only process personal data where a lawful basis applies. The main lawful bases we rely upon are:

- **Contract** – processing necessary to fulfil a booking or agreement.
- **Legal obligation** – e.g. retention of financial records for HMRC.
- **Legitimate interests** – where processing is necessary for the running of the hall, provided it does not override individuals' rights.
- **Consent** – freely given, specific, informed consent, which can be withdrawn at any time.

For "special category data" (e.g. health information), we will obtain explicit consent unless another lawful basis applies.

#### 5. Rights of Individuals

---

Data subjects have the following rights under UK GDPR:

- Right to be informed (via privacy notices)
- Right of access (Subject Access Requests, SARs)
- Right to rectification (correcting inaccurate data)
- Right to erasure ("to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Rights relating to automated decision-making and profiling (not currently used by the Charity)

SARs will be responded to within **one month**. Identity checks will be carried out before releasing data.

## 6. Data Security & Handling Procedures

---

- Personal data will only be accessed by authorised trustees and volunteers.
- Paper records will be stored securely in locked storage.
- Electronic records will be password-protected and backed up securely.
- Portable devices containing data must be encrypted and stored securely.
- Emails containing personal data must be handled with care and deleted when no longer required.
- Accident book entries will be stored securely and reviewed regularly.

## 7. Data Retention

---

Personal data will not be kept longer than necessary. Typical retention periods:

- **Financial records** – 7 years
- **Hirers' booking records** – 2 years after last booking
- **Accident reports** – 3 years (or until child is 25 if involving a minor)
- **Employee/volunteer records** – 6 years after leaving (longer if required for pensions, safeguarding, or insurance)
- **Minutes and legal documents** – kept indefinitely as part of the charity's archive

## 8. Data Breach Reporting

---

Any trustee, volunteer or contractor who becomes aware of a personal data breach must report it immediately to the Data Protection Lead.

- All breaches will be recorded in a **Data Breach Log**.
- Where a breach poses a risk to individuals' rights or freedoms, the ICO will be notified within **72 hours**.
- Data subjects will be informed where the breach is likely to result in a high risk to them.

## 9. Sharing of Data

---

Personal data will not be shared with third parties unless:

- Required by law
- Necessary to fulfil a contract or service (e.g. with insurers, contractors, or funding bodies)
- With the explicit consent of the individual

## 10. Responsibilities of Trustees, Volunteers and Staff

---

Everyone handling personal data must:

- Read and comply with this policy
- Only access data necessary for their role
- Keep data secure at all times
- Report any suspected breach immediately

Failure to comply may result in removal from their role and, in serious cases, legal action.

## 11. Review and Updates

---

This policy will be reviewed **biennially** or sooner if there are changes in legislation, guidance, or operational practice.

**Version 2 adopted by the Management Committee:** Tuesday, 26 August 2025

**Date for Next Review:** Wednesday, 26 August 2026