Failand Village Hall

Registered Charity Number 304540

Failand Village Hall GDPR & Data Protection Policy

1. Introduction

This GDPR & Data Protection Policy explains how the Failand Village Hall ("the Hall") collects, uses, stores, and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Hall is committed to respecting the privacy of all hirers, volunteers, trustees, employees, contractors, and members of the public.

2. Purpose of this Policy

This policy ensures that the Hall:

- Handles personal data lawfully, fairly, and transparently
- Collects only the data necessary for its operations
- Stores data securely
- Retains data only for as long as needed
- Disposes of data securely when no longer needed
- Responds appropriately to data rights requests
- Demonstrates accountability and good governance

3. Scope

This policy applies to all personal data processed by the Hall, including:

- Booking information
- Financial and accounting records
- Volunteer and trustee details
- CCTV footage
- Emails and correspondence
- Accident and incident reports

It covers data relating to hirers, volunteers, trustees, contractors, and members of the public. held in both paper and digital formats.

4. Roles and Responsibilities

Data Controller

The Hall's Management Committee acts as the Data Controller and is responsible for ensuring compliance with UK GDPR.

Committee Members and Volunteers

All individuals handling personal data must:

- Follow this policy
- Keep data secure
- Report any data breaches immediately

5. Lawful Bases for Processing

The Hall processes personal data under the following lawful bases:

Purpose	**Lawful Basis**
Managing bookings and hire agreements	Contract
Financial management and accounting	Legal obligation
Accident reporting and insurance	Legal obligation / legitimate interest
Governance and trustee management	Legal obligation
CCTV for security	Legitimate interest
Mailing lists and marketing	Consent
Volunteer management	Legal obligation

6. Types of Data Collected

The Hall may collect:

- Names, addresses, phone numbers, email addresses
- Booking details and hire agreements
- Payment information (not stored beyond processing)
- Accident/incident information
- CCTV images
- Volunteer/trustee details
- Emails and correspondence

The Hall does **not** collect unnecessary or excessive data.

7. How Data Is Used

Personal data is used only for legitimate Hall purposes, including:

- Managing bookings and enquiries
- Maintaining financial records
- Ensuring safety and security
- Communicating with hirers and volunteers
- Meeting legal and regulatory obligations

The Hall does **not** sell or share data with third parties except where legally required (e.g., insurers, HMRC).

8. Data Storage and Security

The Hall will ensure that:

- Paper records are stored in locked cabinets
- Digital records are password-protected and backed up
- Booking, financial and or accounting systems are password-protected and where appropriate, backed up
- Access is restricted to authorised Management Committee members only
- Devices used for Hall business have appropriate security measures
- Data is disposed of securely (shredding, secure digital deletion)

9. Review of Data

- The Hall will review its records **annually** to identify data that should be deleted in line with this policy.

10. Data Retention

The Hall retains data only for as long as necessary. A full retention schedule is described in Section 17.

11. Data Subject Rights

Individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request deletion where appropriate
- Withdraw consent (for consent-based processing)
- Object to certain types of processing
- Lodge a complaint with the Information Commissioner's Office (ICO)

Requests should be submitted to the Management Committee via the Data Protection Officer (see below for contact details), who will respond within one month.

12. Data Breaches

A data breach includes loss, theft, unauthorised access, or accidental disclosure of personal data.

If a breach occurs:

1. It must be reported immediately to the Management Committee.
2. The Management Committee will assess the risk using the ICO Self-assessment tool.
3. Serious breaches will be reported to the ICO within 72 hours.
4. Affected individuals will be informed where required.

13. CCTV

Where CCTV is used:

- It is for security and crime prevention
- Footage is retained for a short, defined period (see Section 16)
- Access is restricted
- Signage is displayed to inform the public

14. Children's Data

Where data relates to children (e.g., accident reports), the Hall will take extra care to ensure:

- Minimal data is collected
- Data is stored securely
- Retention periods follow legal requirements (e.g., until age 21)

15. Contact Details

- For the attention of the Data Protection Officer via FailandVillageHall@gmail.com
- Or by post to;

  The Data Protection Officer
  Failand Village Hall
  Oxhouse Lane
  Failand
  North Somerset
  BS8 3TS

16. Review of Policy

This policy will be reviewed every **two years**, or sooner if legislation or operational needs change.

17. Retention Schedule

The following retention periods reflect legal requirements, regulatory guidance, and the operational needs of the hall.

17.1 Booking and Hire Records

Data Type	Retention Period	Reason
Booking forms, hire agreements, contact details	**6 years**	Contractual limitation period; audit trail
Emails relating to bookings	**Up to 2 years**, unless linked to financial records	Operational need

17.2 Financial and Accounting Records

Data Type	Retention Period	Reason
Invoices, receipts, bank statements, accounts	**6 years**	HMRC requirements
Gift Aid declarations	**6 years after last donation**	HMRC requirement

17.3 Governance and Trustee Records

Data Type	Retention Period	Reason
Trustee contact details, declarations	**6 years after leaving role**	Charity Commission guidance
Annual General Meetings/management committee minutes	**Permanent**	Historical and governance value

17.4 Health & Safety

Data Type	Retention Period	Reason
Accident/incident reports (adults)	**3 years**	Limitation period
Accident/incident reports (children)	**Until child turns 21**	Limitation period
Risk assessments	**5 years**	Best practice

17.5 CCTV

Data Type	Retention Period	Reason
CCTV footage	**Maximum 30 days**	Proportionate security use
Footage relating to an incident	**Until investigation concludes**	Legal/insurance need

17.6 Volunteer Records

Data Type	Retention Period	Reason
Volunteer contact details	**While active + 1 year**	Operational need

17.7 Marketing and Communications

Data Type	Retention Period	Reason
Mailing list subscribers	**Until consent withdrawn**	GDPR consent rules
Photos used for publicity	**Until consent withdrawn**	GDPR consent rules