Martin Village Hall GDPR Policy

Martin Village Hall — Privacy Notice

Martin Village Hall (MVH) is committed to protecting your privacy and handling your personal data securely and transparently in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. Who We Are

Martin Village Hall ("we", "us", or "our") acts as the **Data Controller** for personal data collected in connection with the management, operation, hiring, and events of the Hall.

If you have any questions about this Privacy Notice or how we handle your personal data, please contact:

- **Contact Role:** Chair / Data Protection Lead
- **Email:** martinlincsvillagehall@gmail.com
- **Postal Address:** Martin Village Hall, High Street, Martin, Lincolnshire LN4 3QT

2. What Personal Data We Collect & How We Use It

We collect and process personal data for specific purposes, using the following **lawful bases**:

Purpose	Types of Data Collected	Lawful Basis
Hall Bookings & Hiring Management	Name, contact details (email, address, phone number), payment details/bank information	**Contract:** Necessary to enter into or perform a hiring agreement with you.
Financial & Accounting Records	Invoices, payment records, bank details	**Legal Obligation:** Necessary to satisfy accounting, tax, and audit obligations.
Marketing & Event Updates	Name, email address	**Consent:** Where you have explicitly opted in to receive event updates or newsletters.

Purpose	Types of Data Collected	Lawful Basis
		Legitimate Interests: Where sending updates to existing hirers about hall services.
Promotional Photos & Social Media	Photographs or videos taken at hall events	**Consent:** Explicit permission requested prior to publication.
Volunteer & Trustee Administration	Name, contact information, emergency contacts, DBS check status (where required)	**Legitimate Interests / Legal Obligation:** To administer hall operations and meet regulatory duties.

3. Sharing Your Information

We will **never sell or rent** your personal data to third parties. We may share your data only where necessary and lawful with:

- **Service Providers:** Third-party providers supporting our operations (e.g., online booking platforms, banking systems, cloud storage providers) under strict confidentiality agreements.
- **Legal & Regulatory Bodies:** The Information Commissioner's Office (ICO), HMRC, insurers, or law enforcement if required by law or necessary for legal/insurance claims.

4. Data Retention

We keep personal data only for as long as necessary:

- **Financial & Booking Records:** Retained for up to **7 years** to comply with UK accounting and tax laws.
- **Insurance Records:** Retained for longer periods where required by our insurance policies or legal claims rules.
- **Marketing Lists:** Kept until you withdraw consent or unsubscribe.
- **General Correspondence:** Deleted regularly once no longer required operationally.

5. Your Legal Rights

Under the UK GDPR, you have the following rights regarding your personal data:

- **Right of Access:** Request a copy of the personal data we hold about you (Subject Access Request).
- **Right to Rectification:** Ask us to correct inaccurate or incomplete data.
- **Right to Erasure ('Right to be Forgotten'):** Request the deletion of your data where no overriding legal requirement exists to retain it.
- **Right to Restrict or Object:** Limit or object to our processing of your personal data (including opting out of marketing at any time).

- **Right to Data Portability:** Request transfer of your data to another provider where applicable.

To exercise any of these rights, please contact the Chair. We will respond within **one calendar month**.

6. Complaints

If you have concerns about how we handle your data, please contact us first so we can resolve the issue. You also have the right to lodge a complaint with the UK data protection regulator:

- **Information Commissioner's Office (ICO)**
- **Website:** www.ico.org.uk
- **Helpline:** 0303 123 1113

Martin Village Hall — Internal Data Protection Policy

1. Purpose & Scope

Martin Village Hall (MVH) relies on personal data to manage bookings, facilities, governance, and events. This policy sets out the mandatory rules that all **trustees, officers, and volunteers** must follow to ensure compliance with the **UK GDPR** and **Data Protection Act 2018**.

This policy applies to all forms of personal data held on paper or electronically (computers, mobile phones, email accounts, messaging apps, removable storage).

2. Core Data Protection Principles

All personal data processed on behalf of MVH must be:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified, explicit, and legitimate purposes.
3. Adequate, relevant, and limited to what is necessary (**data minimisation**).
4. Accurate and kept up to date.
5. Kept no longer than necessary (**storage limitation**).
6. Handled with appropriate security (**integrity and confidentiality**).

3. Operational Guidelines for Trustees & Volunteers

A. Storage & Digital Security

- Devices used to process MVH personal data (computers, laptops, mobile phones) must be password- or PIN-protected.
- Anti-virus software and device operating systems must be kept updated.
- Data must not be stored on unencrypted USB sticks or unsecure personal drives.

B. Paper Documents

- Physical hiring contracts, keyholder lists, or paper forms containing personal data must be stored securely (e.g., in locked cabinets/drawers).
- Paper files must be safely shredded once their retention period expires.

C. Email Communications & Newsletters

- **BCC Function:** When sending emails to multiple individuals or mailing lists (other than internal Trustee groups), **always use the 'BCC' (blind carbon copy) field** to prevent disclosure of email addresses.
- Regular mailbox purges must be conducted to delete non-essential emails containing personal information.
- Every marketing/event update email must include an easy option for recipients to unsubscribe or opt out.

D. Data Subject Access Requests (SARs)

- Any request from an individual to access, correct, or delete their personal data must be passed to the Chair immediately.
- Responses must be provided without delay and **within one calendar month**.

4. Data Breaches

A personal data breach includes accidental loss, destruction, alteration, unauthorised disclosure of, or access to personal data.

1. **Immediate Reporting:** Any trustee or volunteer who suspects or discovers a breach must report it immediately to the Chair.
2. **Assessment:** The Chair/Trustees will assess the risk to affected individuals.
3. **ICO Notification:** If the breach poses a risk to individuals' rights and freedoms, MVH must notify the **Information Commissioner's Office (ICO) within 72 hours** of becoming aware of the breach.
4. **High Risk:** If the breach poses a high risk to individuals, those affected must be informed without undue delay.

5. Roles & Responsibilities

- **Board of Trustees:** Overall legal responsibility for UK GDPR compliance lies with the Board of Trustees collectively.
- **Individual Trustees & Volunteers:** Responsible for following this policy during their day-to-day duties on behalf of MVH.

6. Review

This policy will be reviewed annually by the Board of Trustees or whenever data protection legislation changes.

Review

This policy is reviewed regularly and updated as required.

Date revised: 1st August 2026

Next review date: 1st August 2028

Author

Kevin Garner-Smith (Trustee & Treasurer)