LAMPLUGH
VILLAGE HALL

Data Protection Policy

INTRODUCTION

This policy outlines how Lamplugh Village Hall collects, stores, and processes personal data, ensuring compliance with the UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA 2018). This includes recent updates from Data (Use and Access) Act 2025 (DUAA).

The Hall is committed to protecting individuals' rights and freedoms regarding their personal data, and the policy applies to trustees, volunteers, hirers, users, any future staff, and anyone processing data on behalf of the Hall.

This policy covers all personal data processed by the Hall, regardless of format (electronic or paper), including data collected for:

- Hall bookings and enquiries
- Managing Finances and accounts
- Marketing and promoting events
- Fundraising activities
- Any other activities involving personal data.

PRINCIPLES

The Hall adheres to the seven data protection principles:

1. **Lawfulness, fairness, and transparency**: Data will be processed lawfully, and transparently, in a way individuals expect and have been informed about.

2. **Purpose limitation**: Data will be collected and used only for specified, explicit, and legitimate purposes and not further processed incompatibly with those purposes.

3. **Data minimization**: Only the minimum amount of personal data necessary for the stated purpose will be collected and stored.

4. **Accuracy**: Personal data will be accurate, up-to-date, and kept accurate where necessary, with procedures for rectification and erasure.

5. **Storage limitation**: Data will not be kept longer than necessary, considering legal and insurance requirements (e.g. 7 years financial records).

6. **Integrity** and confidentiality (security): Personal data will be stored securely, protected against unauthorized or unlawful processing, accidental loss, destruction, or damage.

7. **Accountability**: The hall will demonstrate compliance with the principles through appropriate measures and record-keeping.

LAWFUL BASES FOR PROCESSING

The Hall will identify and document a lawful basis for processing all personal data. Possible lawful bases include:

• **Legitimate Interests**: Processing is necessary for the Hall's legitimate interests (e.g. managing books, finance).

• **Consent**: Where required, explicit consent will be obtained for specific purposes (e.g. sharing contact details for other groups).

• **Contractual Requirements**: Necessary for fulfilling a contract with the data subject (e.g. booking agreement).

• **Legal Obligation**: Necessary for compliance with a legal obligation (e.g. submitting trustees details to the Charity Commission).

• **Vital Interests**: Necessary to protect someone's life (e.g. health information in emergency situations).

• **Public Task**: Necessary for performing a task in public interest (e.g. consulting local people about neighborhood issues).

INDIVIDUALS RIGHTS

The Hall will respect and uphold individuals; rights concerning their personal data.

• **Right to be informed**: Individuals will be informed why their data is being collected, how it will be used, and their rights through a privacy notice.

• **Right of Access** (Subject Access Request – SAR): Individuals can request a copy of the data held about them. Requests will be dealt with within 30 days.

• **Right of Rectification**: Individuals can have inaccurate or incomplete data corrected.

• **Right to Erasure** (Right to be Forgotten): Individuals can request their data to be deleted where there is no compelling reason for its retention.

• **Right to Restriction of Processing**: Individuals can request to limit how their data is used in certain circumstances.

• **Right to Data Portability**: Individuals can obtain and reuse their data for their own purposes across diPerent services.

• **Right to Object:** Individuals can object to the processing of their data in certain situations.

• **Rights in relation to automated decision making and profiling**: Individuals have rights to decisions made Soley based on automated processing. DATA SECURITY The Hall will implement appropriate technical and organisational measures to ensure data security.:

• **Access Control**: Access to personal data will be restricted to authorised trustees, staP and volunteers.

• **Password Protection**: All devices (computers, laptops, tablets, mobiles etc) used for the Hall business will be password protected.

• **Secure Storage**: Electronic data will be stored in password-protected files, and paper records will be filed securely, preferably in a locked cabinet.

• **Secure Disposal**: When data is no longer needed, it will be securely deleted or destroyed (e.g. permanently deleted from computers, shredding paper documents). • Third-Party Compliance: If storing data online via a third-party website (e.g. google drive), the Hall will ensure the third party complies with UK GDPR.

• **Data Breach Procedures**: Procedures will be in place to handle and report personal data breaches, including reporting to the ICO within 72 hours if there is a risk to individuals.

DATA SHARING

Personal data will not be shared with third parties without the individual's consent, unless there is a lawful basis for doing so, such as a legal requirement or fulfilling a contract.

• When data is shared with another organisation (e.g. payroll, pensions), a binding contract with data processing clauses will be in place.

• When sending emails to multiple recipients, the 'Bcc' field will be used to avoid sharing email addresses with other recipients unnecessarily .

LAMPLUGH
VILLAGE HALL

TRAINING AND AWARENESS

All trustees, staP and volunteers will receive raining on data protection obligations and this policy.

• They will declare compliance with this policy, potentially through signing a confidentiality and data protection agreement.

• Basic training will cover the eight data protection principles, and documentation of this training will be kept.

ROLES AND RESPONSIBILITIES

The Management Committee (Charity Trustees) is ultimately responsible for data protection compliance within the Hall.

• A designated individual may be appointed as a 'Data Protection Contact' responsible for managing data protection issues and acting as the primary contact point for data subjects.

• Specific Individuals (e.g. Booking Secretary, Treasurer) will be responsible for managing the data relevant to their roles.

• All individuals processing data on behalf of the Hall will be aware of the implications of breaching data protection and their potential personal liability for misuse of data.

Date August 2026

Renew Date August 2027