Data Protection Policy and Procedures

1. Introduction

The Data Protection Act 1998 (DPA) and the General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Lavant Memorial Hall (LMH) is a registered charity whose administration necessitates the collection and processing of personal data. The Trustees are committed to a policy of protecting the rights and privacy of individuals and regard the lawful and correct treatment of personal data as very important to successful working and to maintaining the confidence of those with whom LMH deals. The Trustees recognise the risk to individuals of identity theft and financial loss if personal data is lost or stolen. Trustees and any other volunteers or individuals who have access to personal data in the course of administering the hall will therefore be expected to read and comply with this policy.

This policy will be updated as necessary to reflect good practice in data management, security and control and to ensure compliance with any changes in legislation. In case of any queries or questions in relation to this policy please contact the Hall Secretary.

2. Definitions

Act means the Data Protection Act 1998 (DPA) and the General Data Protection Regulations (GDPR) – the legislation that governs the use of personal data.
Data Controller – the Trustees, who collectively decide what personal data LMH will hold and how it will be held and used.
Data Subject – an individual whose personal data is being held or processed by LMH, for example a hirer or donor.
Data Users - Trustees and any other volunteers, individuals and organisations who have access to personal data in the course of administering the hall i.e. the Data Processors
'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of his/her personal data. Explicit consent is needed for processing "sensitive data", which includes:

a) Racial or ethnic origin of the subject
b) Political opinions
c) Religious beliefs or other beliefs of a similar nature
d) Trade union membership
e) Physical or mental health condition
f) Sexual orientation

g) Criminal record
h) Proceedings for any offence committed or alleged to have been committed

LMH does not process "sensitive data" in the normal course of administering the hall.

Information Commissioner's Office (ICO) – the ICO is responsible for implementing and overseeing the Act

Processing – means collecting, amending, handling, storing or disclosing personal data

Personal data/information – information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not include information about organisations, companies and agencies.

Subject Access Request (SAR) - individuals have a right to make a SAR to find out whether LMH holds their personal data, where, what it is used for, to have data corrected if it is wrong and to prevent use that is causing them damage or distress.

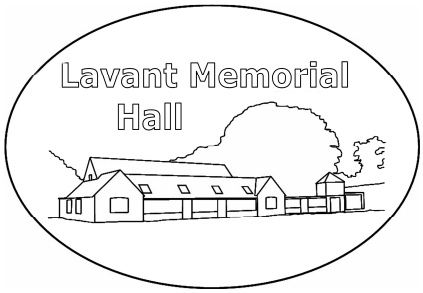
3. Data Processing Principles

The Data Protection Act contains eight principles for processing personal data with which LMH must comply, namely that personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more of the purposes specified in the Act and shall not be processed in any manner incompatible with that purpose(s).
3. Shall be adequate, relevant and not excessive in relation to that purpose(s).
4. Shall be accurate and, where necessary, kept up to date.
5. Shall not be kept for longer than is necessary.
6. Shall be processed in accordance with the rights of Data Subjects under the Act[1].
7. Shall be kept secure by the Data Controller who takes appropriate technical and other means to prevent unauthorised or unlawful processing, and accidental loss or destruction of, or damage to, personal information.

[1] *Note that Data Subjects' rights include:*

a. The right to be informed that processing is being undertaken
b. The right of access to one's personal information
c. The right to prevent processing in certain circumstances, and
d. The right to correct, rectify, block or erase information which is regarded as wrong information.



8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

4. Responsibilities

The Trustees are the Data Controller under the Act and are legally responsible for complying with the Act. The Trustees determine for what purposes personal data held by LMH will be used.

The Management Committee will take into account the legal requirements and ensure, through appropriate management and application of criteria and controls, that:

a) A record is maintained of what, where and how personal data is stored and processed and that this record is updated periodically e.g. on the appointment or retirement of a Data User, and no less often than every 3 years.
b) The eight data processing principles are applied.
c) SARs can be actioned securely and expeditiously. The procedure for handling SARs is set out in Annex 2 to this document.

Individual Data Users who have access to personal data in the course of administering the hall are personally responsible for processing and using such data in accordance with the Act. All Data Users should be aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

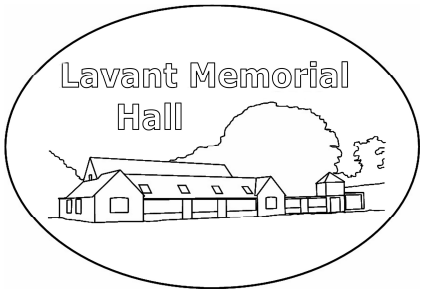
Where LMH relies on a third-party organisation to process personal data e.g. by using hall booking and invoicing software, LMH will ensure that the third-party has appropriate Data Protection and Processing policies that comply with the Act.

Note that LMH is not required by the ICO to appoint a Data Protection Officer and has not done so.

5. Privacy Notice and Consent Policy

LMH publishes the following Privacy Notice on its website (How to Book page) and on the booking form to be used by hirers.

Lavant Memorial Hall uses personal data for the purposes of managing hall bookings, finances and events, publicity, fundraising and for the upkeep and maintenance of the hall facilities. Personal data is also processed by



trusted third-parties solely for the purposes of administering bookings. Personal data will be stored securely and will only be accessible on a need-to-know basis. Information will be stored for only as long as needed, or required by statute, and will be disposed of appropriately.

'Explicit' consents are not required for these purposes. In the event that use of personal data for any other purpose is contemplated then, save in the case of extraordinary SARs as outlined in the operational guidance below, or where the personal data is already in the public domain, 'Explicit' consent will be sought and a record of such consent(s) stored by the Secretary in a securely held electronic or paper file.

6. Procedures for Handling Data & Data Security

Access to personal data will be limited to Data Users on a need-to-know basis. LMH has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

All Data Users must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. Any information (which is not otherwise in the public domain) that can be used to identify an individual must be treated as personal data and subjected to the operational guidance given in Annex 1.

7. Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The ICO must be notified where the breach is likely to result in a risk to individuals: e.g. damage to reputation, financial loss, loss of confidentiality. Clarification must be sought from the ICO helpline (0303 123 1113) if there is doubt as to whether an incident represents a significant breach. A report must be made to the ICO within 72 hours (3 days) of becoming aware that an incident is reportable.

ANNEX 1: Operational Guidance for Data Users

Personal data can be held on computers, laptops and other mobile devices, on portable digital media, or in a manual file, and includes email, minutes of meetings and photographs.

Minutes and Documents:

Where individuals need to be identified in public documents e.g. minutes, and harm may result, initials rather than full names will normally be used.

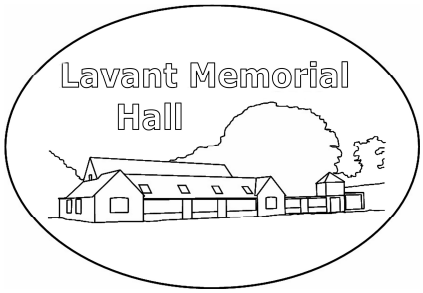
Email:

You should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved in the appropriate folder, or printed and stored securely.
Emails that contain personal information no longer required for operational use should be deleted from the personal mailbox and any "deleted items" box.
Where someone not a trustee, volunteer or contractor needs to be copied into an email e.g. a wider circulation list for an upcoming event, we encourage use of bcc instead of cc, so as to avoid their personal data being shared through forwarding.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous.
- If you have any doubts, ask the caller to put their enquiry in writing.
- If you receive a phone call asking for personal information to be checked, or confirmed, be aware that the call may come from someone impersonating someone with a right of access.



Laptops and Portable Devices:

All laptops and portable devices that hold personal data must be protected with a suitable password that is changed regularly. Where sensitive data or financial information is held an encryption program should be used.

- Ensure your laptop is locked (password protected) when left unattended, even for a short period of time.
- When travelling in a car make sure that the laptop is out of sight, preferably in the boot.
- If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.
- Never leave laptops or portable devices in your vehicle overnight.
- Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.
- When travelling on public transport keep laptops or portable devices with you at all times, do not leave them in luggage racks or even on the floor alongside you.

Data Security and Storage

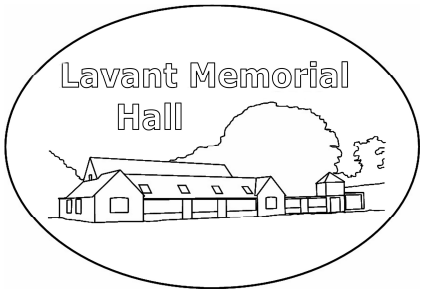
Store as little personal data as possible relating to LMH on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the computer or laptop. The disk or memory stick should then be securely returned (if applicable|) safely stored, or wiped and disposed of securely.

Always lock (password protect) your computer or laptop when left unattended.

Passwords

Do not use passwords that are easy to guess. All your passwords should contain both upper and lower case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length. ***Protect your password*.** Common sense rules for passwords are:

- Do not give out your password.
- Do not write your password somewhere on your laptop.
- Do not keep your password written on something stored in your laptop case.



Data Storage:

Personal data will be stored securely and will only be accessible to legitimate Data Users.

Information will only be stored for as long as it is needed or required by statute and will be disposed of appropriately. For financial records this is up to 7 years. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required, or when Data Users retire.

All personal data held for LMH must be non-recoverable from a computer which has been passed on/sold to a third party.

Accident Book:

The accident book will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely by the Hall Secretary.

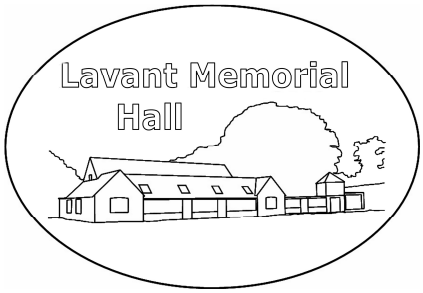
Photography

LMH may use general photographs of events with groups of adults at the hall for publicity purposes in accordance with its lawful basis for using personal data. Photos of children must not be used without the written consent of the parent or guardian. However, LMH is aware that for some individuals publicising their location could place them or their families at risk. Consequently at large events at which publicity photos are to be taken a notice should be posted at the entrance, or an announcement made, providing opportunity for people to refuse taking part in publicity photographs. At small events the consent of individuals (verbal) should be obtained if their image will be clearly identifiable. Hirers are encouraged to comply with this policy

Extraordinary Data Subject Access Requests (SARs)

LMH may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of LMH. The circumstances where the law allows LMH to disclose data (including sensitive data) without the Data Subject's consent are:

a) Carrying out a legal duty or as authorised by the Secretary of State protecting vital interests of a Data Subject or other person e.g. child protection.
b) The Data Subject has already made the information public



c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
d) Monitoring for equal opportunities purposes – i.e. race, disability or religion

In any other circumstances a consent to share personal data must be obtained from the data subject(s).

ANNEX 2: Procedure for Handling SARs

Background

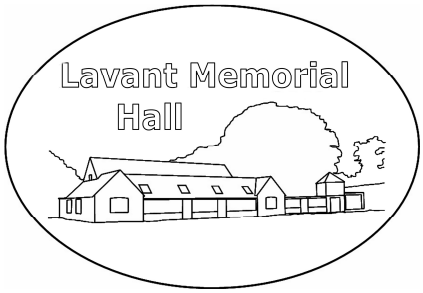
The Act strengthens the rights of individuals to obtain confirmation from an organisation as to whether or not personal data concerning them is being used, where and for what purpose. This is called a Subject Access Request (SAR). A copy of the personal data has to be provided, free of charge unless the request is 'manifestly unfounded or excessive', in an electronic format, including any emails where they are mentioned. If the data was not obtained from that individual, details of where it came from have to be provided. Individuals also have a number of other rights, of which the two most likely to be relevant to village halls are, the right to have data rectified if incorrect or incomplete and to have data erased where there is no compelling reason for it to continue to be held.

There is a 30 day time limit in which to respond and certain information that must be provided. However, before providing the information the individual's identity must be verified to avoid the possibility of a data breach. An extension of time can be requested if there is good reason e.g. holiday, illness.

Given the relative simplicity of personal data processing undertaken by LMH (as set out in our Privacy Notice), most SARs are likely to be straightforward. However, it is possible for more complex scenarios to arise and the Act does not specify how an individual must lodge a request (they can be made verbally for example). Consequently, this procedure will concentrate on recognizing and recording SARs, establishing their legitimacy, setting a timescale, assigning responsibility for responding, and identifying the information that must be consulted in framing a response.

Procedure

1. LMH will recognize a SAR made by an Applicant to any Officer, Trustee or the Booking Secretary (the Recipient).



2. The Recipient shall immediately notify the Hall Secretary and Chairman with a copy of the SAR. If the SAR was verbal the Hall Secretary shall write/email the Applicant re-iterating the SAR and seeking confirmation that it has been correctly understood. The Hall Secretary shall log the SAR, open a file and set the response timescale, which starts from the day following initial receipt of the SAR.
3. As soon as the SAR is clear the Officers shall review it and decide
    a. Whether there is any doubt as to the identity of the Applicant. If so, their identity must be confirmed by reference to photo ID (e.g. passport, driving licence) and proof of address (e.g. recent utility bill, bank or credit card statement) to avoid the possibility of a data breach.
    b. Whether the SAR is 'manifestly unfounded or excessive' – if in doubt advice should be sought from the ICO as to whether to refuse, charge a fee and/or extend the timescale.
    c. Whether the Applicant should be asked for longer to comply if there is good reason e.g. holiday, illness.
    d. Who should coordinate the response, a named trustee – the Coordinator.
4. The Coordinator should consult the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/, which sets out detailed guidance in respect of complying with individuals' rights under the Act, and determine the scope and form of the response.
5. The Coordinator shall notify all Trustees and the Booking Secretary of the SAR, the personal data affected, the action required of them and the timescale applicable (the LMH GDPR Data Mapping Questionnaire responses may be used for guidance). It will be for the Coordinator to assess whether any third parties need to be included in this exercise.
6. All those so notified shall affirm in writing that they have complied with the Coordinator's request.
7. The Coordinator shall:
    a. ensure that a record of all steps taken and outcomes is placed on file
    b. compile a response to the SAR
    c. alert the Officers if the response timescale is at risk
8. The Officers shall review and approve the response before release to the Applicant.