Data Protection (GDPR) Policy

1. Introduction

The purpose of this Policy is to ensure that Howard Hall Memorial Hall complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all other applicable data protection legislation when processing personal data.

2. Responsibilities

The Management Committee recognises that protecting personal data is essential to maintaining the trust and confidence of hall users, volunteers, contractors, and the wider community. The Committee is responsible for ensuring that Howard Hall Memorial Hall complies with the requirements of the UK GDPR and related legislation.

The Management Committee will review this Policy and the Hall's data protection arrangements every two years, or sooner where there are changes to legislation, new systems are introduced, or operational practices are significantly amended.

The Hall Secretary shall oversee day-to-day compliance with this Policy and shall act as the first point of contact for data protection enquiries.

3. Key Principles

Howard Hall Memorial Hall is committed to processing personal data in accordance with the principles of the UK GDPR. Personal data shall be:

a. collected only where it is necessary for the effective operation and management of the Hall, including the administration of the booking system;
b. adequate, relevant and limited to what is necessary for the purposes for which it is processed;
c. processed lawfully, fairly and transparently
d. accurate and, where necessary, kept up to date;
e. retained only for as long as necessary to fulfil the purposes for which it was collected or to meet legal, regulatory or contractual requirements;
f. processed securely using appropriate technical and organisational measures;
g. protected against unauthorised or unlawful access, alteration, disclosure, loss or destruction; and
h. processed in a manner that enables Howard Hall Memorial Hall to demonstrate compliance with the requirements of the UK GDPR.

4. Supporting Documents and Guidelines

This Policy is supported by the following documents:

a. The Hall GDPR Privacy Notice;
b. Records of Processing Activities;

c. Data Retention Schedule; and
d. Data Breach Procedure, see Appendix.

5. Data Security

The Hall shall ensure that access to personal data is restricted to those individuals who require such access to fulfil their duties and responsibilities.

Personal data collected for the administration of Hall bookings shall be protected by appropriate technical and organisational measures designed to safeguard its confidentiality, integrity and availability. These measures include; the use of a web application firewall, regular vulnerability monitoring, secure authentication controls, anti-malware protection, and the timely application of security updates.

Individuals authorised to access personal data shall use strong, unique passwords, maintain appropriate endpoint security, and comply with the Hall's information security requirements.

Personal data shall be retained and securely disposed of in accordance with the Hall's Data Retention Schedule.

6. Subject Rights

The Hall shall respond to requests from individuals exercising their rights under the UK GDPR within the statutory timescales. Such rights include the right to access, rectify, erase, restrict or object to the processing of personal data, where applicable.

7. Data Breaches

The Hall Secretary shall manage the initial response to the breach and, where appropriate, consult the Management Committee and any appointed Data Processor. The Management Committee will in conjunction with the Data Processor:

a. assess the breach;
b. minimise any risks;
c. maintain a breach log;
d. notify the Information Commissioner where legally required;
e. inform affected individuals where appropriate.

A record of the incident and actions taken will be recorded using the Data Breach form, included as an Appendix to this Policy.

8. Training

Committee members, volunteers and any other individuals who process personal data on behalf of the Hall shall receive appropriate guidance and, where necessary, training to ensure they understand their responsibilities under this Policy and applicable data protection legislation.

Version	Data Protection (GDPR) Policy Version 1
Date Approved	25 August 2026
Approved By	Howard Hall Management Committee
Responsible Officer	Hall Secretary
Supporting Framework	Data Protection Framework
Related Documents	Privacy Notice Record of Processing Activities (ROPA) Data Retention Schedule and Terms Conditions of Hire
Review Date	August 2030

Appendix A – Data Breach Register

Date of Breach: _____ Date Reported _____

Reported by: _____ Reported to: _____

Description of the Breach
Provide a brief description of the incident, including how the breach occurred.

Personal Data Involved
Describe the categories of personal data affected (e.g. names, addresses, email addresses, telephone numbers, booking information).

Number of Individuals Affected

Initial Containment Actions
Describe the immediate actions taken to contain the breach and prevent further unauthorised access or disclosure.

Risk Assessment

ICO Notification

Was the ICO notified? If Yes, Date and Time of Notification:
☐ Yes ☐ No

Notification to Affected Individuals

Were affected individuals notified? If Yes, Date of Notification:
☐ Yes ☐ No ☐ Not Required

Corrective Actions
Describe any corrective actions taken to prevent a recurrence.

Closed

By: _____ Position: _____

Date: _____ Signature: _____