Hawkesbury Hospital Hall

Charity Number 1176993

GDPR Policy

This policy has been adopted by Hawkesbury Hospital Hall Management Committee who remain responsible for its biennial review.

Date: October 2023

Review Date: October 2025

Hawkesbury Village Hall

Privacy Notice

Hawkesbury Hospital Hall aims to ensure full compliance with the General Data Protection Regulation (GDPR) and aims to care for personal data appropriately. The Regulations apply to data in digital form and in hard copy, and mean that:

- Data needs to be processed securely
- Data needs to be updated regularly and accurately
- Data must be limited to what the organisation needs
- Data must be used only for the purpose for which it is collected and
- Before using personal data, organisations must give people clear information about how it will be used.

The Committee will never pass on or sell personal information and will not hold data unnecessarily.

1. Why this policy exists

This policy ensures that the hall:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers, volunteers, trustees, and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risk of a data breach.

2. Data protection law

The Data Protection Act 1998 describes how organisations — including the Hall — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant, and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

3. Responsibilities

Everyone who works or volunteers for or with the Hall has some responsibility for ensuring data is collected, stored and handled appropriately.

All staff and volunteers must ensure that personal data is handled and processed in line with this policy and data protection principles.

The Committee of Trustees is ultimately responsible for ensuring that the Hall meets its legal obligations. It is also responsible for:

- Keeping itself updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.

- Handling data protection questions from staff and volunteers and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the Hall holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the Hall's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the Hall is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff or volunteers to ensure marketing initiatives comply with data protection principles.

The committee may appoint a nominated data protection trustee to assist with these responsibilities.

4. General guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**.
- **The Hall will provide training** to all staff, trustees, and volunteers to help them understand their responsibilities when handling data.
- All staff, trustees and volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used,** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the organisation or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- All staff, trustees and volunteers **should request help** from the chair or nominated data protection trustee if they are unsure about any aspect of data protection.

5. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the chair or nominated data protection trustee.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Staff, trustees, and volunteers should make sure paper and printouts are **not left where unauthorised people could see them**, such as on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts. As the Hall does not have its own IT system, these rules apply to the storage of data by staff, trustees, and volunteers on their own IT devices:

- Data should be **protected by strong passwords** that are changed regularly and never shared between staff, trustees and volunteers.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to **approved cloud computing services**.
- Data should be **backed up frequently**.

6. Use of data

It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, staff, trustees, and volunteers should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. It should never be sent by email, as this form of communication is not secure.
- Personal data must **never be transferred outside the European Economic Area**.

7. Accuracy of data

The law requires the Hall to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all staff, trustees and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. No-one should not create any unnecessary additional data sets.
- Staff, trustees, and volunteers should **take every opportunity to ensure data is updated.**
- Data should be **updated as inaccuracies are discovered**.

8. Subject access requests

All individuals who are the subject of personal data held by the Hall are entitled to:

- Ask **what information** the Hall holds about them and why.
- Ask **how to gain access** to it.

- Be informed **how to keep it up to date.**
- Be informed how the Hall is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the chair, or nominated data protection trustee.

Individuals will be charged £10 per subject access request. The chair or nominated data protection trustee will aim to provide the relevant data within 14 days.

The chair or nominated data protection trustee will always verify the identity of anyone making a subject access request before handing over any information.

9. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Hall will disclose requested data. However, the chair or nominated data protection trustee will ensure the request is legitimate, seeking assistance legal advice where necessary.

10. Why we need personal information

Personal information is needed to run the Committee of Trustees, comply with charity law, pay staff, reimburse trustees and volunteers and to facilitate bookings and enable hirers to be invoiced. A full schedule of the uses of information is set out in Appendix A.

11. The Committee - Procedure for Use and Retention of Personal Information

To ensure we operate in a way that complies with the requirements of legislation, we will comply with the following procedure:

i). After the AGM, each Committee member will be asked if their name, email address and telephone number can be shared with other Committee members.

ii) Committee members will be asked if their name and the organisation they represent can be listed on the website. After the AGM, an updated list of Committee Members will be displayed on the website.

iii) If a Committee Member leaves the Committee during the year or if they wish to withdraw their consent, the Secretary will inform other Committee Members and ask them no longer to contact the individual regarding Hall Business, and to remove their details from any electronic devices or paper records that they hold.

iv) If Bank Details are required, these will be requested by the Treasurer, who will remind the individual that:

- Details of their bank account and sort code will be held with the Hall Bank Account.
- Their name and information about payment(s) will be held in our Financial Records.

v). If information is required for the Charity Commission this will be requested by the Treasurer.

Each year, the list of Committee Members will be updated by the Secretary to ensure it includes only current members. Individuals who have left the Committee will therefore no longer have their details included on the list.

Copies of the minutes are retained and kept securely.

Individuals who have left the committee will immediately have their details removed from our banking account, but records showing historic transactions may still refer to them.

12. Hirers - Procedure for Use and Retention of Personal Information

As the provider of a Village Hall for hire, we need to hold some information in order to meet legal contractual requirements. This information is collected through the Booking Form that is available on our website and completed by the Hirer.

The information we collect is: name, email address and telephone number.

We use this information to communicate with the hirer, to ensure that the booking goes smoothly and to enable us to collect payment.

The information is entered onto the bookings system by the Bookings Secretary. Access to the system is password-protected and is only available to the Bookings Secretary and Treasurer. The information will be retained for 2 years from the date of the booking taking place.

13. What to do if you have any questions

If you have any questions, please contact the Secretary.

If you are dissatisfied, you have a right to raise a complaint with the Information Commissioner's Office at www.ico.org.uk

Appendix A – GDPR Data Usage & Retention Policy

Type of data	Subject	Reason for processing	Legal basis	Retention period
Name, address, dob, NINO, pension details, pay history, tax, NI	Staff	Legal requirement to fulfil HMRC and Pension Regulator's rules and to process pay and pension contributions and to assess pension, tax and NI liability	Legal obligation	Duration of employment
Name, address, dob, NINO, pension details, pay history, tax, NI	Former Staff	Legal requirement to fulfil HMRC and Pension Regulator's rules and to process pay and pension contributions and to assess pension, tax and NI liability	Legal obligation	7 years after leaving
Bank details	Staff	To enable payment of wages direct to bank accounts	Consent	Duration of employment
Bank details	Former Staff	To enable payment of any outstanding wages or entitlements to bank accounts	Consent	1 year after leaving
Attachment of earnings order	Staff	To enable deduction from wages and payment to the relevant authority	Legal obligation	Duration of employment
Attachment of earnings order	Former Staff	To enable deduction from wages and payment to the relevant authority	Legal obligation	7 years after leaving
Holiday entitlement and usage	Staff	To ensure staff have their correct entitlement to paid holiday	Consent	Duration of employment
Holiday entitlement and usage	Former Staff	To ensure staff have their correct entitlement to paid holiday	Consent	3 years after leaving

Type of data	Subject	Reason for processing	Legal basis	Retention period
Sickness information including reasons for illness, medical certificates and self-certificates and periods of absence	Staff	To manage staff absence	Contract	Duration of employment
Sickness information including reasons for illness, and periods of absence	Former Staff	To enable the provision of accurate information on reference requests	Consent	3 years after leaving
Sickness information including periods of absence	Former Staff	To satisfy legal requirements on SSP	Legal requirement	7 years after leaving
Email address	Staff	To enable sending payslips, pension information and training materials	Consent	Duration of employment
Email address	Former Staff	To enable sending payslips and pension information	Consent	2 years after leavin
Name, address, former employment details, dob, qualifications	Job applicants	To enable consideration of job applications and to prove fair consideration	Consent	1 year after position filled
Nationality and residence status	Job applicants	To comply with the law on entitlement to work	Legal requirement	7 years after appointment
Name, address, dob	Trustees	Required by Charity Commission	Legal requirement	1 year after resignation
Name, bank account details	Trustees	To enable repayment of expenses	Consent	1 year after resignation
Name, organisation	Trustees	Public awareness of identity of the trustees – details appear on website	Consent	Duration of trusteeship

Type of data	Subject	Reason for processing	Legal basis	Retention period
Name	Trustees	Minutes of meetings	Legal requirement	To be kept for life of the organisation.
Name, address, email address	Hirers	To make bookings and process invoices and payments	Consent	3 years after booking
Name, address, email address, phone number	People making a complaint	To address issues raised in a complaint	Consent	2 years after complaint closed.
Name and organisation	Hirers	To display in the on-line bookings calendar	Consent	6 months after booking
Name, address, dob, contact details	People reporting accidents	To retain accident information and allow reporting under RIDDOR where necessary	Legal requirement	5 years. In the case of serious accidents involving children, until the child reaches 21 years of age
CCTV images	Visitors, hirers, staff, volunteers, trustees, members of the public	Crime prevention, public safety, to provide evidence	Consent and/or legal requirement	Data is overwritten after 30 days.