



DITTON PRIORS HALLS GDPR POLICY

Introduction

This Policy explains how Ditton Priors Village Halls Committee (the Committee) collects, uses, stores and protects personal data in accordance with the Data Protection Act (1998) and UK General Data Protection Regulation (GDPR) legislation. Our focus is on ensuring that personal data is treated lawfully and correctly.

Personal data is any information that relates to an identifiable individual, such as name, address, contact details, age, gender, and family details. Personal data can be lawfully obtained for the purposes of managing the Halls – e.g., bookings, finances, invoicing, trustee and committee member information. Personal data must be held securely, only used for the legitimate purpose for which it was collected, and disposed of when no longer required.

Our charities are registered with the Information Commissioner's Office (ICO) (<https://ico.org.uk>) and we pay an annual subscription. All committee members and trustees are aware of the 7 data protection principles as set out on the ICO website (see [Appendix A: Data Protection Principles](#)).

How do we use personal data?

We use personal data for the following purposes and only to the extent needed:

- To manage Halls bookings and events
- To respond to enquiries about bookings and events
- To maintain financial and administrative records
- To comply with legal and regulatory requirements
- To send updates or information about events, maintenance, meetings, etc.

What information do we collect?

For the purposes of managing the Halls, we collect the following personal data about our trustees, committee members, volunteers, hirers, suppliers and membership of our clubs/activities:

- Names
- Addresses
- Email addresses
- Telephone numbers

We have 2 dedicated email addresses, as follows:

- info@dittonpriorshalls.co.uk for general enquiries
- dittonpriorshalls@gmail.com for booking enquiries

All committee members and trustees must use blind copy (BCC) for emails to multiple recipients.

Emails received or sent that contain personal data are either deleted if no longer required, or saved to the appropriate folder if retained as an official record.

We have a dedicated mobile phone which stores names and telephone numbers.

We have a website which publishes contact information for our regular activities.

At the Village Hall, we record CCTV footage – refer to the Ditton Priors Village Hall CCTV Policy.

Our accident books are located in each Hall. They are checked periodically and appropriate action taken.

How do we store personal data?

Everyone holding personal data must have secure password protection on all their devices and have internet security installed.

We use an online shared platform to store shared files – including policies, invoices, photographs of events, etc. – and we use an online shared calendar to record information about bookings, meetings and events.

We store paper files at the Village Hall in a locked office. This may include information about our suppliers and ongoing maintenance contracts (which may also include financial information) and some archive material.

Paper files are also held by the Treasurer when appropriate and some personal data may be stored on spreadsheets by an officer of the committee for the purposes of managing the Halls and our activities.

Personal data is retained for only as long as necessary, but may be retained for up to 7 years for accounting purposes, and for longer where required by our insurers.

When do we share personal data?

Personal data obtained for legitimate purposes can be shared in order to facilitate management of the Halls. Access is limited to trustees and committee members.

The Committee will *not* share personal data with third parties unless:

- Specific consent has been given
- It is in the public domain
- An exemption applies, such as a safeguarding issue or as required by law or regulation (e.g., for insurance purposes)

In case of a data breach

A personal data breach may lead to the destruction, loss, alteration, unauthorised disclosure of – or access to – personal data.

We are required to report some types of data breach to the ICO, normally within 3 days of the occurrence. Specifically, we are required to notify the ICO where this is likely to result in a risk to individuals – e.g., damage to reputation, financial loss, loss of confidentiality.

If a device is stolen or hacked and risk to individuals may result, the breach should be reported to the ICO. This also applies to paper files.

In the event of a data breach, we will review our processes to avoid a recurrence.

Consent forms

Explicit consent is required for processing personal data. Processing includes collecting, amending, storing and disclosing information.

Consent forms are distributed and signed annually and stored securely by the Bookings Secretary.

Subject Access Requests

Under GDPR legislation, individuals have the right to request a copy of all personal data held about them – a Subject Access Request (SAR) – by contacting the Committee by email (info@dittonpriorsfalls.co.uk). We would first verify the identity of the applicant by requesting proof of name and address and then provide any information we hold in electronic format within 30 days.

Individuals have the right to have incorrect or incomplete data rectified.

Complaints

Complaints regarding the implementation of this policy or the refusal of a SAR will be addressed as per the Ditton Priors Halls Complaints Procedure.

The Committee is aware that a data breach may lead to action being taken against them.

Review

The Committee will review this Policy periodically or when there are significant changes in the law or our practices.

Contact Details

Ditton Priors Village Halls Committee email: info@dittonpriorsfalls.co.uk.

Appendix A: Data Protection Principles

Below are the 7 key data protection principles, as set out in the ICO website:

1. **Lawfulness, fairness and transparency:** You must process personal data lawfully, fairly, and in a transparent manner by being clear and open with individuals from the start.
2. **Purpose limitation:** You must only collect personal data for specified, explicit, and legitimate purposes, and not process it in a way that is incompatible with those purposes.
3. **Data minimisation:** You must ensure that personal data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
4. **Accuracy:** Personal data must be accurate and, where necessary, kept up-to-date, with every reasonable step taken to erase or rectify inaccurate data without delay.
5. **Storage limitation:** You must keep personal data in a form that permits identification of individuals for no longer than is necessary for the purposes for which it is processed.
6. **Integrity and confidentiality (security):** You must process data in a manner that ensures appropriate security, protecting it against unauthorised or unlawful processing, accidental loss, destruction or damage.
7. **Accountability:** You are responsible for complying with these principles and must be able to demonstrate your compliance.