

Data Protection Policy

The Hiltingbury School Parents and Teachers Association (HSPTA) commitment to protecting privacy and data forms a key policy for the Committee. This policy underpins both this Data Protection Policy and other associated policies used by HSPTA. It is important to note that as Data Controllers any Committee member or volunteer is responsible for personal data they process and must therefore ensure that they are aware of their responsibilities under the law.

This policy sets out HSPTA's approach to protecting personal data and explains your rights in relation to how we may process personal data.

If you have any queries about anything set out in this policy, please write to committee.hspta@gmail.com.

We may from time to time make minor changes to this policy. We will notify you directly when we make any substantial or significant changes to the policy.

Some Important Definitions

'ICO' is the Information Commissioner's Office, the body responsible for enforcing data protection legislation within the UK and the regulatory authority for the purposes of the GDPR

'Personal Data' is defined below

'Processing' means all aspects of handling personal data, for example collecting, recording, keeping, storing, sharing, archiving, deleting and destroying it.

'Subject Access Request' is a request for personal data that an organisation may hold about an individual. This request can be extended to include the deletion, rectification and restriction of processing.

What is personal data?

Personal data means any information about an identified or identifiable person. For example, an individual's home address, personal (home and mobile) phone numbers and email addresses, and so on can all be defined as personal data.

Some categories of personal data are recognised as being particularly sensitive ("special category data"). These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic and biometric information, medical information, and data concerning a person's sex life or sexual orientation.

How does data protection apply to HSPTA?

Data protection legislation applies to all data processors regardless of whether they are charities or small organisations.

HSPTA is a registered Charity and they collect and store personal data about customers, for example, they are data controllers and must adhere to the law.

What type of personal data do we collect and why?

Customer Data

Personal data about our customers is held on the pta-events website. We believe it is important to be open and transparent about how we will use your personal data. Information held about you may include name, address, contact details, purchase history and payment details.

We need this information to communicate with you about events you have bought tickets to.

We also use this information to distribute marketing and newsletters to those that have opted into this service. These can be opted into and out to at any time through the website and the 'unsubscribe link' at the bottom of emails.

All this information is collected by you directly entering it on the website.

Donors

We benefit from donations from members of the public who support our work, and we hold personal data (Name, Address) about these donors so that we can process donations and complete the gift aid declaration as required by HMRC.

Event Specific Information

Some events require additional personal information (e.g.: class name). Sometimes this includes special category information such as medical information about allergies. This information is required to make sure the events run smoothly and safely.

This information is gathered by you entering information onto the website when completing forms for individual events.

Conditions for collecting personal data

We must keep to the law when processing personal data. To achieve this, we must meet at least one of the following conditions:

- **Consent** - you must give (or have given) your permission for us to use your information for one or more specific purposes
- **Performance of a contract** - we need to process the information to meet the terms of any contract you have entered (for example when we process personal data as part of a volunteer's membership application or to provide goods or services purchased with us)
- **Legal obligation** - processing the information is necessary to keep to our legal obligations as data controller
- **Vital interests** - processing the information is necessary to protect your vital interests
- **Public task** - processing the information is necessary for tasks in the public interest or for us as the data controller to carry out our responsibilities
- processing the information is necessary for our legitimate interests (see below examples)

Lawful basis	Data processing examples
Consent	<ul style="list-style-type: none">• Sending marketing information and Newsletters.• Volunteer contact details
Performance of a contract	<ul style="list-style-type: none">• Supply of goods or services purchased
Legal obligation	<ul style="list-style-type: none">• Responding to information requests from statutory authorities

Vital interests	<ul style="list-style-type: none"> Allergy or medical condition disclosure to a medical professional to protect the vital interests of the data subject
Public task	<ul style="list-style-type: none"> HSPTA will use other more appropriate lawful basis for processing personal data
Legitimate in-interest	<ul style="list-style-type: none"> Informational/operational communications directly to volunteers*

Also, information must be:

- processed fairly and lawfully
- collected for specified, clear and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- processed securely

Information that we share

We do not share personal data with companies, organisations and people outside the HSPTA unless one of the following applies;

- We have a clear lawful basis to do so.
- If we have to supply information to others for processing on our behalf. If we do this, we make sure that they are keeping to the GDPR and have appropriate confidentiality and security measures in place.
- For other legal reasons.

A list of the most common third parties we share personal data with can be found below:

3 rd Party	Data Category	Purpose
PTA Events Ltd	Personal and Special	Management and maintenance of the pta-event platform
NCPTA Enterprises Ltd	Personal and Special	Management and maintenance of the pta-event platform
HMRC	Personal	Gift aid declarations
Google	Personal	Surveys and Provision of HSPTA core data repository
SumUp	Personal	Payment gateway for online fundraising transactions
Stripe	Personal	Payment gateway for online fundraising transactions

Keeping personal data secure

Everyone who handles personal data (including committee members, volunteers and third-party providers) must make sure it is held securely to protect against unlawful or unauthorised processing and accidental loss or damage. We take appropriate steps to make sure we keep all personal data secure, and we make all of our committee members aware of these steps. In most cases, personal data must be stored in appropriate systems and encrypted when taken off-site. The following is general guidance for everyone involved with HSPTA

- You must only store personal data on networks, drives or files that are password protected and regularly backed up.
- You should keep paper records containing personal data secure. If you need to move paper records, you should do this strictly in line with data protection rules and procedures.
- You should not download personal data to mobile devices such as laptops and USB sticks unless necessary. Access to this information must be password protected and the information should be deleted immediately after use.
- Personal data relating to members and volunteers should usually only be stored on the pta website or google drive which have appropriate security in place.
- When sending personal data by email this must be appropriately authenticated and password protected.
- Do not send financial or sensitive information by email unless it is encrypted.
- You should not share your passwords with anyone.
- Different rights of access should be allocated to users depending on their need to access personal or confidential information. You should not have access to personal or confidential information unless you need it to carry out your role.
- Before sharing personal data with other people or organisations, you must ensure that they are GDPR compliant.
- In the event that you detect or suspect a data breach, you should follow your defined breach response process.

All committee members undertake annual training to ensure that they are aware of the above rules. Any event leads are also trained.

Data Retention

We may keep information for different periods of time for different purposes as required by law or best practice. Individual departments include these time periods in their processes. We make sure we store this in line with our Data Retention Policy

Rights to accessing and updating personal data

You are entitled to ask us, in writing, for a copy of the personal data we hold about you. This is known as a subject access request (SAR). In line with legislation, we will not charge a fee for this information and will respond to your request within one calendar month.