# PANT MEMORIAL INSTITUTE - DATA PROTECTION POLICY

**Contents**



References: 1) ACRE Information Sheet 4 (Copy available to trustees on request.)

## 1) INTRODUCTION

We need to collect and use certain types of information in order to carry on our work of managing Pant Memorial Institute. This personal information must be collected and handled securely, to protect the rights and privacy of individuals.

The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The trustees and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. **All trustees and volunteers will therefore be expected to read and comply with this policy.**

## 2) DEFINITIONS

The purpose of this policy is to set out the Pant Memorial Hall commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen. The following are definitions of the terms used:

- Data Controller - the trustees who collectively decide what personal information Pant Memorial Institute will hold and how it will be held or used.
- Act means the Data Protection Act 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.
- Data Protection Officer – the person responsible for ensuring that Pant Memorial Institute follows its data protection policy and complies with the Act. As a small charity Pant Memorial Institute is exempt from appointing a specific DPO. Any enquiries should be directed to the secretary.
- Data Subject – the individual whose personal information is being held or processed by Pant Memorial Institute, for example a donor or hirer.
- 'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him. Explicit consent is ESSENTIAL for processing "sensitive data", which includes:
    - Racial or ethnic origin of the data subject

- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Criminal record
- Proceedings for any offence committed or alleged to have been committed

- Information Commissioner's Office (ICO) - the ICO is responsible for implementing and overseeing the Data Protection Act 1998.
- Processing – means collecting, amending, handling, storing or disclosing personal information.
- Personal Information – information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

## 3) PRINCIPLES OF THE DATA PROTECTION ACT

This contains 8 principles for processing personal data with which we must comply. 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 or those purposes,
3) Shall be adequate, relevant and not excessive in relation to those 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,
7) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal 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) CORRECTING DATA

Individuals have a right to make a Subject Access Request (SAR) to find out whether the charity holds their personal data, where, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them. Any SAR must be dealt with within 30 days. Steps must first be taken to confirm the identity of the individual before providing information, requiring both photo identification e.g. passport and confirmation of address e.g. recent utility bill, bank or credit card statement.

## 5) RESPONSIBILITIES

Pant Memorial Institute is the Data Controller under the Act, and is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for. **As the charity has no legal identity of its own, this responsibility devolves to the trustees**.

The management committee will take into account legal requirements and via the procedures listed in section 6, will do the following:

a) Collect and use information fairly.
b) Specify the purposes for which information is used.
c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
d) Ensure the quality of information used.
e) Ensure the rights of people about whom information is held, can be exercised under the Act. These include:

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

f) Take appropriate technical and organisational security measures to safeguard personal information,
g) Ensure that personal information is not transferred abroad without suitable safeguards,
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
i) Set out clear procedures for responding to requests for information.

**All trustees and volunteers must be aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.**

Pant Memorial Institute has a duty to ensure that appropriate technical and organisational measures are taken to prevent:

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

All trustees and volunteers must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA. It is therefore important that all trustees and volunteers consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data, and observe the guidance given below.

## 6) OPERATIONAL GUIDANCE

### a) Applying the Data Protection Act and GPDR within the charity

We will let people know why we are collecting their data, which is for the purpose of managing Pant Memorial Hall, its hirings and finances. It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to trustees and volunteers.

The charity website includes its own privacy policy and general data protection statement.

## b) Use of Committee Details

The charity provides a set of public contact details which may be freely shared outside the committee and volunteers. These are:

- The postal address of the hall: Pant Memorial Hall, Pant, Oswestry, Shropshire SY10 9QG
- The email address for bookings: bookings@pantmemorialhall.org.uk
- The email address for the secretary: secretary@pantmemorialhall.org.uk
- The email address for the treasurer: treasurer@pantmemorialhall.org.uk
- The booking mobile: 07913 565708
- The facebook page: @pantmemorialhall
- The twitter account: @pantmemhall

The names of the trustees are also listed on the Charity Commission website. The Charity Commission holds trustee addresses and dates of birth, but these details are not publicly visible.

NO other contact details of trustees or volunteers shall be given to anyone outside the committee, i.e. anyone not listed on the contact list maintained by the secretary and provided to all committee members and volunteers. The protected details include surnames, home addresses, telephone numbers (landline or mobile) and personal email addresses.

## c) Email

The public email addresses listed above should be used by the officers concerned to communicate with those outside the committee. Communications within the committee may use personal email addresses but these are to be kept in confidence.

All trustees and volunteers 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 into the appropriate folder or printed and stored securely. Emails no longer required should be deleted.

## d) Phone Calls

Phone calls can lead to unauthorised use or disclosure of personal information. 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. Refer also to item b) above.
- If you have any doubts, ask the caller to put their enquiry in writing (including email).
- 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.

## e) Laptops and Portable Devices

**All laptops and portable devices that hold data containing personal information must be protected with a strong password. The password should not be kept near the device.**

Ensure that your laptop or device is locked (password protected) when left unattended, even for short periods of time. Laptops and devices should be appropriately protected, especially if removed from the home. All data relating to the charity must be non-recoverable from any device being sold on or destroyed.

## f) Data Security and Storage

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Take care with disks or memory sticks used to transfer data, and ensure they are safely stored or wiped/destroyed if no longer required.

## g) Data Storage

Personal data will be stored securely and will only be accessible to authorised trustees or volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. Data storage times are defined in the separate Financial Policy.

## h) Guidance for booking secretary

Completed hiring forms should be kept in a dedicated file and are subject to all the security guidance given above. Any forms received electronically should be kept only in the booking secretary email account. Hiring forms need to be kept for 10 years, but should be destroyed after that date.

Family events (e.g. birthday parties, anniversary celebrations, wakes etc) will be listed on the online calendar simply as 'private booking'. No other details should be entered on to the calendar, even if they are not set to be visible.

## i) Accident Book

This takes the form of separate pages held in the Health and Safety folder. Any page which has been completed will be removed, appropriate action taken and the page filed securely.

## j) Data Subject Access Requests

We 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 the charity. The circumstances where the law allows the charity 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

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

## k) Risk Management

The consequences of breaching Data Protection can cause harm or distress to hall users and committee members if their information is released to inappropriate people. Trustees and volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks, and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.