Hale Village Hall New Forest (CIO)

Charity Registration Number 1175048

DATA PROTECTION POLICY 2024

Hale Village Hall Management Committee needs to keep certain information about its trustees, volunteers and service users to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring that any personal data will be dealt with in line with the EU General Data Protection Regulation (GDPR) 2016. To comply with the regulation, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures.

In line with the GDPR 2016 principles, we will ensure that personal data will:

- Be obtained fairly and lawfully and for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures

Hale Village Hall Management Committee processes the following personal information:

See attached Data Map

- Trustees - Names, addresses, email addresses, dates of birth, telephone numbers
- Film Club, Table Tennis Club, 100 Club members - Names and contact details
- Suppliers, contractors, hirers and payees – Names, contact details, bank details

Hale Village Hall Management Committee will ensure that:

- Data will not be sold to companies or given to public organisations. Personal data (names, addresses, emails, phone numbers) will only be passed on to a third party with written consent (e.g. someone who wants to contact someone else who does want their information public)
- Be processed for the purposes stated only.
- In the case of contact details, these may be stored for the purpose of informing the community about events, activities etc, but this will not include personal information other than that which has been permitted and an opt-out option will apply.
- Be accurate and be kept up to date
- Be erased as soon as out of date or when not necessary
- Be kept in a safe place and, where relevant, on a computer which is password protected.

The information regarding any individual will be available for them to view on demand, subject to proof of their identity.

Responsibilities

Hale Village Hall Management Committee is the Data Controller under the Act and is legally responsible for complying with the Act. The Management Committee will take into account the legal requirements and ensure that it is properly implemented.

Procedures for handling Data and Data Security

The Management Committee has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

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

All trustees, staff 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.

Email - All trustees, staff 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.

Phone calls - 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.

Laptops - All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password).

Data Security and Storage –

- Only essential personal data should be kept.
- Personal data received on disk or memory stick should be saved to the relevant file on the laptop, the disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.
- Personal data will be stored securely and will only be accessible to authorised volunteers or staff.
- Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.
- All personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party

Data Subject Access Requests (SAR) – There may occasionally be a 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:

- 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
- The Data Subject has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes - i.e. race, disability or religion

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Trustees, staff 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.

All organisations are required to report certain types of data breach to the ICO and in some cases to the individuals affected. A report to the ICO must be made within 72 hours (3 days) of becoming aware that an incident is reportable.

Ring the ICO's helpline 0303 123 1113 for clarification if you are unsure whether something represents a significant breach.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. You only have to notify the ICO where it is likely to result in a risk to individuals: For example, damage to reputation, financial loss, loss of confidentiality. If a data breach occurs, it is important to check whether anything could be done to avoid it happening again.

All trustees, employees and volunteers need to be aware that it is essential that any PC, laptop, mobile, tablet, CD or memory stick used for village hall purposes is password protected and that if any of these items are stolen or hacked, and risk to individuals results, the breach is reported. The same applies to paper files.

Policy Review

The Management Committee will review this policy on a three yearly basis or earlier if conditions change or there is a change in statutory demands.