St Johns Village Memorial Hall Association

Registered Charity no: 1139761 Registered in England no: 7313464

Data Protection Policy

St Johns Village Memorial Hall, Festival Path, St Johns Lye, Woking, Surrey GU21 7SQ

Version 2: May 2018

Context and overview

Key details: The policy seeks to outline the St Johns Village Memorial Hall Association's (SJVMHA) commitment to complying with Data Protection law, outlining the roles and responsibilities for the committee, volunteers and employees of the association and users of the hall facility.

Policy prepared by	Fiona Nadin, Mike Ness
Approved by board of management on:	21 May 2018
Policy became operational on:	25 May 2018
Next review date:	March 2020

Introduction

St Johns Village Memorial Hall Association (SJVMHA) needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards - and to comply with the law.

The Appendix describes how this policy is used in practice

Why this policy exists

This data protection policy ensures that SJVMHA

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

Data protection law

The Data Protection Act (1998) and the General Data Protection Regulations (GDPR) operative from 25 May 2018 describe how organisations - including St Johns Village Memorial Hall Association 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 and GDPR are 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 to be held longer than necessary

6. Processed in accordance with the rights of data subjects.

7. Be protected in appropriate ways

8. Not to be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities

Policy Scope

- This policy applies to The St Johns Village Memorial Hall Association
- All staff and volunteers of the St Johns Memorial Hall association
- All contractors, suppliers and other people working on behalf of St Johns Village Memorial Hall Association
- All users of the St Johns Village Memorial Hall

The policy applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act (1998) and GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Sensitive information relating to individuals such as employment history, equality and diversity information, DBS information and health related information such as medical conditions, allergy and the like.

Data protection risks

This policy helps to protect SJVMHA from some very real data security risks, including:

- Breaches of confidentiality. For instance, information given out inappropriately.
- Failing to offer choice. For instance all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

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

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

General Staff 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. When access to confidential information is required, employees and volunteers of the association can request it from the management committee.

SJVMHA will provide training to its employees and volunteers to help them understand their responsibilities when handling data.

Employees and volunteers should keep all data secure, by taking sensible precautions and following guidelines below.

- In particular, strong passwords should be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company 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 disposed of or deleted.
- Employees and volunteers should request help from the committee if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored.

- 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 are kept in a locked drawer or filing cabinet.
- Employees and volunteers should make sure that paper and printouts are not left where unauthorised people could see them, like on a printer. This also applies to individuals, groups and businesses hiring the hall spaces.
- Data printouts should be shredded and disposed of securely when no longer required

However, these people have key areas of responsibility:

The trustees of the memorial hall association are ultimately responsible for ensuring that the association meets its legal obligations.

The hall committee is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issue
- Reviewing all data protection policies and related policies in line with an agreed schedule
- Arranging data protection training and advice for people covered in this policy
- Handling data protection questions from anyone covered by this policy
- Dealing with requests from individuals to see the data that the association holds about them (also called 'subject access requests').
- Checking and approving and contracts or agreements with third parties that may handle the company's sensitive data.

The Hall Manager.

In addition to the responsibilities held by the committee, the hall manager is responsible for:

- Ensuring that the management committee are updated on any data protection risks and issues.
- 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 third party services that the company is considering using to store or process data. For instance, cloud computing services.
- The hall manager with the support of the hall management committee is responsible for approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets like newspapers
- Where necessary working with other staff and volunteers of the association to ensure marketing initiatives abide by data protection principles.
- In addition, the hall manager, when data is stored electronically, must ensure that data. Is protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees or volunteers of the association.
- 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 be stored in designated drives and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the association's standard back up procedure.
- Data should never be saved directly on to laptops or other mobile devices such as smart phones

- All servers or computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is no value to SJVMHA unless the business can make use of it. However, 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, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Personal data should never be transferred outside the European Economic Area
- Employees should not save copies of personal data to their own computers.

Data accuracy law requires SJVMHA to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort SJVMHA should put in to ensuring its accuracy

It is the responsibility of all employees and volunteers working directly for SJVMHA to take reasonable steps to ensure it is kept accurate and as up to date as possible

Data will be held in as few places as necessary. Staff should not create unnecessary additional data sets.

Staff and volunteers of the association should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call,

SJVMHA will make it easy for data subjects to update the information that is held by SJVMHA about them.

Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the data base.

Subject access requests

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

- Ask what information the co any 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 company is meeting its data protection obligations.
- If an individual contacts the SJVMHA requesting this information, this is called a subject access request.
- Subject access requests from individuals should be made by email or in writing and addressed to the data controller (in this instance the hall manager).
- Individuals will be charged £10 per subject access request. The data controller will endeavour to provide the relevant data within 14 days.
- The data controller will always verify the identity of anyone making a subject access request before handing any information.

Disclosing data for other reasons

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

Under these circumstances SJVMHA will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the committee and legal advisors where necessary.

Providing information

SJVMHA aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

The Appendix to this Data Protection Policy shows how the policy is applied in practice including the privacy statement on the web site .

APPENDIX

St John's Village Memorial Hall Association (SJMVHA) Data Protection Policy and GDPR in Practice

SJMVHA only uses data freely given by potential hirers of St John's Memorial Hall as the basis of a hire contract. SJVMHA does not collect or use data from other sources. SJVMHA does not hold sensitive data. SJVMHA does not pass details provided by hirers to other organisations except when required for legal or audit purposes.

SJVMHA holds details of booking enquiries and bookings actually made for St John's Memorial Hall on a bookings database, email archives, accounting package and computer spreadsheets. Paper copies of hire agreements, invoices and bookings confirmations issued to hall hirers are kept for audit purposes.

SJVMHA only collects and holds sufficient information on hirers and potential hirers of the hall to contact the hirer by email post or phone, prepare a hire agreement, check the proposed hire does not conflict with other users of the hall and is within the terms of the hall premises licence. Generally the information is provided by the hirer using the booking enquiry page on the hall web site but may be supplemented by telephone post or email contact.

Access to the data held is normally restricted to the hall/bookings manager and treasurer. Other trustees may deputise when necessary. The hall/bookings manager normally prepares a list of bookings for the trustee or other person on duty at the weekend. The list includes name of hirer, contact details and other special requirements.

The hall/bookings officer acts as Data Controller for the bookings database and the treasurer acts as Data Controller for other data processing. Data processing is normally by the controllers. SJVMHA does not have a Data Protection Officer. Any queries/requests in respect of GDPR should be addressed in the first instance to the Secretary (secretary@stjohnsmha.co.uk)

SJVMHA hires web space and email services from 1&1 and 123-REG. Web pages are maintained By SJVMHA. They do not use cookies. The bookings database is backed up on Dropbox, other files are periodically backed up on removable media. Computers used by SJVMHA are protected by anti-virus software and password protected login.

SJVMHA maintains a paper list of members of the Association in order to establish the right to vote at AGMs.

Privacy Policy

The booking enquiry page of StJohnsMemorialHall.co.uk web site includes a Privacy Statement

"By submitting this booking enquiry you agree that St Johns Village Memorial Hall Association (SJVMHA) can hold the information you provide on a database and contact you by email, phone or post for all purposes associated with hiring a hall, including making a booking, checking for conflicting hires, completing hire agreements and collecting payments.

We will not pass details you provide to any other organisation except when required for legal or audit purposes."

and the line immediately above the submit request button.

"I agree to SJVMHA holding this information and contacting me to process a booking based on this enquiry. "