GDPR4 - Privacy Statement / Data Protection Policies and Procedures / Data Retention Policy & Individual Rights

Introduction

New data protection legislation governing the use of personal data comes into effect on 25th May 2018, these are known as the General Data Protection Regulations (GDPR).

Personal data, such as that used by the Stelling Minnis Village Hall Management Committee, comprises only data that relates to an identifiable individual, such as name, address and contact details. Such data can be lawfully obtained for the purposes of managing the hall e.g. arranging bookings and managing finances. Also, personal data may be shared among Village Hall Committee Members, or with other organisations, solely for the purposes of managing the Hall. Personal data cannot be shared with third-parties unrelated to management of the hall.

The Village Hall Committee does not gather or use highly sensitive personal data such as racial or ethnic origin, health and medical information and sexual orientation. Additionally, since all payments to third-parties are made by cheque, we do not gather financial information such as bank account numbers or sort codes.

Privacy Notice

The Management Committee of the Stelling Minnis Village Hall uses personal data (e.g. name and contact details) which is normally collected only for the legitimate purpose of managing the Hall, its bookings and finances, running and marketing events at the Hall, maintenance and services, and fundraising activities. Data may be retained for up to 7 years for accounts purposes and for longer where required by external authorities (e.g. the Hall's insurers). If you would like to find out more about how we use your personal data or want to see a copy of information about you that we hold, please contact the Hall Secretary.

Data Protection Policy and Procedures

Stelling Minnis Village Hall Management Committee (SMVHMC) (Charity no. 1077969)

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data in order to carry on our work of managing SMVH. This personal information must be collected and handled securely. 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 fie, and includes email, minutes of meetings, and photographs. The Charity will remain the data controller for the information held. The trustees, committee members, staff and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, committee members, staff and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

The purpose of this policy is to set out the SMVHMC commitment and procedures for protecting personal data. 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 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 committee who collectively decide what personal information SMVHMC 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 Subject – the individual whose personal information is being held or processed by SMVHMC.
Explicit consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him.
Information Commissioner's Office (ICO) - the ICO is responsible for implementing and overseeing the Data Protection Act 1998 and General Data Protection Regulations.
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.

The GDPR 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.

We will let people know why we are collecting their data, which is for the purpose of managing [the 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, committee members, staff and volunteers.

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 will 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.

The SMVHMC is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines for what purposes personal information will be held. The management committee will take into account legal requirements and ensure that it is properly implemented and will, through appropriate management, strict application of criteria and controls:

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 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:

1. The right to be informed that processing is undertaken.
2. The right of access to one's personal information.
3. The right to prevent processing in certain circumstances.
4. The right to correct, rectify, block or erase information which is incorrect.

f) Take appropriate technical and organisational security measures to safeguard personal data.

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, committee members, staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

Data Retention Policy

This policy covers the storage and erasure or destruction of personal data.

Personal data will be stored securely and will only be accessible to Committee Members or authorised volunteers or staff. Information will be stored for only as long as it is needed or required in order to manage hall bookings; to maintain contact with users of the hall or with those who service and maintain the hall; and to prepare documentation for year-end financial reporting.

Archival material such as minutes and legal documents will be stored indefinitely. Financial records will be stored for up to seven years. Important archived documents such as deeds, minute books etc. and historical archive material will be kept securely in a locked filing cabinet in a known location.

All other materials, in hard-copy or electronic format, (e.g. invoices, hire agreements, correspondence, emails) will be disposed of appropriately when no longer required or when trustees, staff or volunteers retire or stand down

Names, email addresses, and telephone numbers will be removed from address books, email accounts, or other social media unless this information is for personal, domestic or recreational purposes or the individual has provided consent to share it or it is in the public domain.

All personal data held for the organisation will be rendered non-recoverable from any computer which has been passed on or sold to a third party.

Your Individual Rights

The General Data Protection Regulations (GDPR) strengthen the rights of individuals to obtain information from an organisation as to whether or not personal data concerning them is being used, where and for what purpose. If the data was not obtained from that individual, details of where it came from have to be provided.

Your rights include:
i) The right to be informed that processing is undertaken.
ii) The right of access to one's personal information.
iii) The right to prevent processing in certain circumstances
iv) The right to correct, rectify, block or erase information which is regarded as wrong information or for which there is no compelling reason for it to continue to be held

A copy of the personal data has to be provided, free of charge, unless the request is "manifestly unfounded or excessive".

This is called a Subject Access Request (SAR). The Village Hall Committee has 30 days in which to respond. However, before providing the information we must verify the individual's identity otherwise we could be committing a data breach. We can ask for both photo identification e.g. passport, and confirmation of address e.g. recent utility bill, bank or credit card statement.

Any SAR must be dealt with within 30 days. The website of the Information Commissioner's Office (ICO) shows the information that we must supply (www.ico.org.uk). There are, however, exceptional circumstances in which the law allows us to share your data without consent.

For example, we may 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 without the data subject's consent are:
a) Carrying out a legal duty, or as authorised by the Secretary of State, or protecting vital interests of a Data Subject or other person e.g. as regards 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.

We intend to ensure that personal information is treated lawfully and correctly.