The Watmough Memorial Hall

Charity number: 521979

Also known as: **Saxilby Village Hall** (Working Name)

Data Protection Policy

Document Review History

Data Protection Policy and Procedure – Approved September 2019

Document Ref: SVH/DPP

Status: approved

Version: 1

Date of approval: 23/06/2026

Date of next review: June 2028

Version Control:

Version:

Amended by: Secretary

Details of amendments:

None

Data Protection Policy

Saxilby Village Hall Manage Committee understands and recognises its responsibility to comply with the following:

Data Protection Act 2018 (DPA).
Data Protection Act 2018 - GOV.UK
This is the primary legislation governing data protection in the UK. It updates and replaces the previous Data Protection Act 1998.

The Act controls how personal information is used, ensuring that individuals' data is handled responsibly and securely.

Key features include:

- the rights of individuals regarding their personal data
- obligations for data controllers and processors
- provisions for data breaches

UK General Data Protection Regulations (UK GDPR)

The UK GDPR is a data protection framework that ensures individuals' rights and organisational accountability by governing how personal data of UK residents is collected, processed and protected.

The purpose of this policy:
To set out the Saxilby Village Hall commitment and procedures for protecting personal data. The Management Committee regard the lawful and correct treatment of personal information as the upmost importance 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 mis-used, lost or stolen.

The following are definitions of the terms used:

- Data Controller - the Management Committee who are responsible what personal information Saxilby Village Hall will hold and how it will be held or used.
- Act means the Data Protection Act 2018
- UK GDPR means UK General Data Protection Regulations
- Data Protection Officer (DPO) – the person responsible for ensuring that Saxilby Village Hall Management Committee follows its data protection policy and complies with the Act. Note Saxilby Village Hall is not required to appoint a DPO.

- Data Subject – the individual whose personal information is being held or processed by/for/under Saxilby Village Hall.
- 'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him.
  Explicit consent is needed for processing "sensitive data", which includes:
  i. Racial or ethnic origin
  ii. Political opinions
  iii. Religious or philosophical beliefs
  iv. Trade union membership
  v. Genetic data
  vi. Biometric data used for identification
  vii. Health data
  viii. Data concerning a person's sex life or sexual orientation
  ix. Criminal convictions and offences
- Information Commissioner's Office (ICO): The ICO is responsible for enforcing the Data Protection Act 2018 and the UK GDPR.
- 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 Data Protection Act - This contains 7 core principles that organisations must follow when handling personal data.
  1. Personal data must be processed **lawfully, fairly, and transparently**. Organisations must have a valid legal basis for processing data, inform individuals about how their data will be used, and ensure that processing does not mislead or harm them.
  2. Data should be collected for **specified, explicit, and legitimate purposes** and not used in ways incompatible with those purposes. Exceptions exist for archiving, research, or statistical purposes, provided safeguards are in place.
  3. Only data that is **adequate, relevant, and necessary** for the intended purpose should be collected and processed. This principle prevents excessive or irrelevant data collection.
  4. Personal data must be **accurate and kept up to date**. Organisations are required to correct or delete inaccurate data without delay to maintain reliability.
  5. Data should be **kept no longer than necessary** for the purposes for which it is processed. Longer retention is allowed only for archiving, research, or statistical purposes, with appropriate safeguards.

6. Organisations must ensure **appropriate security** of personal data, protecting it against unauthorised or unlawful processing, accidental loss, destruction, or damage. Measures may include encryption, anonymisation, and access controls.
7. Data controllers are responsible for **demonstrating compliance** with the DPA 2018. This includes maintaining records, implementing policies, and being able to show that all principles are followed in practice.

Applying the Data Protection Act within the charity

We will let hirers/users/staff/volunteers/committee members of the Village Hall know why we are collecting their data - which is for the purpose of managing the hall, its hirings, management and finances. It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to Manage Committee members, staff and volunteers.

Personal data can be held on computers, laptops and mobile devices, or in a manual file. It also includes information contained in, but not limited to minutes of meetings, booking forms, email, social media, WhatsApp and photographs. This can include names, addresses, telephone numbers and email addresses.

Individuals have a right to make a Subject Access Request (SAR) to access any personal information that is held about them. A SAR must be submitted in writing by either hard copy or email). Any SAR must be responded to free of charge and within 30 days, however steps must first be taken to confirm the identity of the individual before providing information, this can be obtained by requiring both photo identification (e.g. passport) and confirmation of address (e.g. recent utility bill, bank or credit card statement). If the individual requests to see data held about them, the SAR response must include:

- How, where, what purpose personal data it is processed and used for
- The time length the data is kept
- Anyone who has access to the personal data

If a SAR includes other individuals' personal data, this must not be disclosed without the permission of the individual for the information to be shared with the data subject, otherwise their personal information must be redacted.

Individuals have the right (under specific rules) to:

- Have incorrect data rectified
- Request their data is erased
- Request the processing of their data is restricted
- Object to their data being processed

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 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:

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, and
IV. 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 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.

a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice

b) Everyone processing personal information is appropriately trained to do so

c) Everyone processing personal information is appropriately supervised

d) Anybody wanting to make enquiries about handling personal information knows what to do

e) Dealing promptly and courteously with any enquiries about handling personal information

f) Describe clearly how the charity handles personal information

g) Will regularly review and audit the ways it holds, manages and uses personal information

h) Will regularly assess and evaluate its methods and performance in relation to handling personal information.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the DPA 2018 and UK GDPR

Procedures for Handling Data & Data Security:

Saxilby Village Hall 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 committee members, staff and volunteers must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies regardless of whether the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone).

Saxilby Village Hall Management Committee will act as the data controller for the information held. The Management Committee, staff and volunteers are personally responsible for processing and using personal information in accordance with the DPA and UK GDPR. The Management Committee, staff and volunteers who have access to personal information will therefore be expected to read and comply with these policies.

Confidentiality:

Management Committee, staff and volunteers must understand that when queries or complaints are made, they remain confidential unless the subject gives permission otherwise. The handling of personal data must remain confidential.

People booking the Hall or contracted to do work for the Hall will make their booking or agree their contract with the Booking Secretary. Information regarding name(s), address and payment method will be passed to the Treasurer. The information given will be collected and processed in accordance with the procedures defined above. Consent forms will be stored by the Booking Secretary in a securely held electronic or paper file.

Operational Guidance

- Email - All committee members, 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. Emails that contain personal information no longer required

for operational use, should be deleted from the personal mailbox and any "deleted items" box.

- Phone Calls - Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:
    a) Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous.
    b) If you have any doubts, ask the caller to put their enquiry in writing.
    c) 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.
- Laptops and Portable Devices:
    i. All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password).
    ii. Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.
    iii. When travelling in a car, make sure the laptop is out of sight, preferably in the boot.
    iv. If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.
    v. Never leave laptops or portable devices in your vehicle overnight.
    vi. Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.
    vii. When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.

Always lock (password protect) your computer or laptop when left unattended.

Passwords:

Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters, a number and special character. Ideally passwords should be 9 characters or more in length.

Protect Your Password - Common sense rules for passwords are:

- Do not give out your password

- Do not write your password somewhere on your laptop
- Do not keep it written on something stored in the laptop case

Personal data will be stored securely and will only be accessible to authorised personnel. Information will be stored for only as long as it is needed or required by statute and when no longer needed, will be shredded or securely disposed.
Archival material such as minutes and legal documents will be stored indefinitely.
Financial records will be for at least 7 years.
Accident records will be for at least 3 years.
General personal files are usually kept up to 6 years after employment/role ends.
Customer records are kept for the duration of the customer relationship, then a further 6 years to cover limitation periods for claims.
CCTV footage is retained for 30days – unless footage is required for a specific incident, in which case it is kept for as long as needed for that investigation or legal claim.

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

Accident Book:
This will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely.

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 (eg 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.

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. Committee members, 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 Saxilby Village Hall is not damaged through inappropriate or unauthorised access and sharing.

Policy Review:

This Data Protection Policy shall be reviewed every two years by the Management Committee and updated as necessary.