SHIMPLING VILLAGE HALL

Essential Data Protection and Information Security for Committee Members

Please read this brief guide to help you understand the background and principles of data protection law and how to follow them in your role as a village hall management committee member.

Introduction
In the UK, data protection is governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

As an organisation, people entrust us with their personal data. We have a legal and moral obligation to keep this information secure. It's not always easy. We are all vulnerable to data breaches or cyber-attacks, whether accidentally sending personal data to the wrong person or clicking on the link of a scam email and putting data security at risk.
We must ensure that data protection and information security are a default in our daily lives to protect individuals' privacy, the data we are responsible for and the village hall's reputation.

Data protection
Data Protection legislation applies to all personal data processed by automated means (such as computer systems like digital communications including email, social media, and telephone call recordings) or by manual processing, which forms part of a 'paper filing system' (any paper records which are structured in some way, such as in chronological, alphabetical or numerical order).

Personal Data includes any information relating to an identifiable living person, known as the Data Subject. For the village hall, this could typically include name, email or postal address, or phone number.

Special Categories means physical or mental health information (including accessibility or dietary requirements), racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union membership, information about an individual's sex life or sexual orientation, genetic or biometric data (where used for ID purposes – e.g. to unlock a device). We must be cautious when processing this type of personal information. Misuse of this type of data could significantly impact an individual's fundamental rights and freedoms, causing them personal distress, financial loss or even risk of physical harm.

Sensitive Data, such as information about children or adults at risk, criminal convictions, gender identity, or financial data such as bank account details, also needs extra care when being processed.

UK GDPR
Six UK GDPR principles must be followed.
These principles are all equally important and ensure that we treat other people's information with the same respect we would want our own to be treated.

Under UK data protection legislation, we must also keep records of our personal data processing activity—this is known as accountability.
Before you begin any new activity involving the processing of personal data, you must understand how to follow the requirements and principles.

1. **We must be transparent, fair and lawful in our processing of personal data.** This means we must tell people what we are doing with their information and why. We must have a valid reason (lawful basis) to process their personal data. For example, if we intend to send people information about an event, we must get their consent and tell them we will do this first. This consent can be granted verbally or in writing.
2. **We must only process people's personal data for a specific purpose or purposes.** For example, we can't collect information for one reason and then use it for another.
3. **We must limit the information we collect to what is adequate and relevant.** We only collect what we need, no more and no less than is necessary for the purpose for which we collected it.
4. **We must ensure that personal information is accurate and up to date in our systems and paper records,** including when requested by an individual.
5. **We must only retain information for as long as necessary for the specific purpose for which it was collected.** We don't keep people's information just because it may be useful one day.
6. **We must ensure we keep personal information secure.** Part of this principle is providing appropriate data protection awareness, using passwords to access systems, and ensuring places where information is viewed is private and are physically safe from intrusion. If you handle personal information in your role, **please look after it**.
Speak to the secretary (DPO) if you have any queries or concerns.

Individual legal rights
Under the UK GDPR / DPA, we all have more information rights and freedoms. This means that the Village Hall is now obliged by law to respond directly to an individual exercising one of their legal rights unless there is a valid reason not to (exemption).
• **The right to be informed.** We must tell people what we are doing with their personal information.
• **The right of access.** If asked, we must provide people with the personal information we have about them.
• **The right to rectification.** If someone's personal data isn't correct, they can now demand we amend this.
• **The right to restriction.** If required, we may need to stop processing people's information for a period.
• **The right to erasure.** People can ask for their information to be deleted unless there is good reason for us not to.
• **The right to object.** People have the right to object to our processing of their information, including for marketing.

If you receive any verbal or written request that you think may be an individual exercising one of their rights, please get in touch with the Data Protection Office (Secretary) as soon as possible. They will then help you to deal with it.

Personal data breach
Under UK GDPR, we must notify the Information Commissioner Office (ICO) about specific types of personal data breaches within 72 hours. So, any potential breach must be reported to the DPO (Secretary) immediately. A personal data breach can take many forms - if you are unsure, please ask and the DPO (Secretary) who will help you assess the incident.
Examples of a personal data breach may include:
• Losing an event attendee list or anything that holds attendees contact details.
• Sending an email that displays personal email addresses in the "To" or "Cc" field to group of people. (use shimplingvh@gmail.com instead or ensure **"Bcc"** is used for email).
• Publishing images of identifiable people enjoying a recent event without a signed model / media release form.

Our top tips for staying data protection compliant in your role at the village hall:
1. Always use shimplingvh@gmail.com when emailing groups or residents - it is more secure than using personal email and will prevent email addresses from being accidentally disclosed.
2. Do not use unauthorised personal devices to process personal information.

If you have any questions, please get in touch with the Data Protection Officer (Secretary).

The village hall management committee is by constitution responsible for the general management organisation letting and control of the use of the hall for the purpose of entertainment recreation and social gatherings or otherwise to benefit of the inhabitants of the Parish and adjacent parishes.
To do this, we need to process personal data of people. This personal information is entrusted to us. We do not "own" it and must protect it by following the law. You have an essential role in looking after this information - if we treat other people's information with the care and respect that you would want your information to be treated with, then we won't go far wrong.

Information Security
Classifying and handling information
Using sensitivity labels, we classify information into two levels: **Confidential** and **General**. This helps us manage data storage, sharing, and printing.
• **Confidential**: accessible only to authorised individuals. Unauthorised disclosure could seriously harm the village hall. Examples include personal data, payment card data, and third-party contacts.
• **General**: available to anyone without restriction. Examples include non-sensitive internal information like event details, how-to guides, and policies.

Creating, editing, and storing
Label Confidential information (paper and electronic). No label is needed for General information.
• **Paper Copies**: lock away Confidential papers when not in use. Remove them from the hall premises only if necessary and always secure them.
• **IT Systems**: store documents in agreed apps and password protect confidential information

Sharing and sending
Ensure proper agreements (Data Processing/Non-disclosure/Confidentiality) are in place before sharing or sending **Confidential** information. Do **not** send paper documents unless there is a genuine business need to do so – where possible, use an electronic method instead.
Confidential paper information must be sent via tracked or postal methods. Check that the recipient is authorised to receive information & the address is correct.
If you use IT systems, ensure documents are shared via the village hall email account

For printing, copying and scanning, only use personal printers when you are present and can remove the documents immediately after creation.

Disposing
General information should be recycled or deleted when no longer needed.
Confidential information must be disposed of either:
- In **Confidential** waste bins.
- Shredded in a Cross shredder.
- Deleted and deleted /removed from the computer recycle bin

Passwords
Never share or write down passwords outside the management committee. Create strong passwords using easy-to-remember but hard-to-guess passphrases, random words, or personal mnemonics (e.g. purplesunflower).
For best practice:
• Use unique passwords for each account and avoid sequential changes (e.g., GiantsCauseway1 to GiantsCauseway2).
• Enable Multi-Factor Authentication (MFA) for added security.
• Avoid personal information in passwords (e.g., birthdays).

Physical security
Please be aware of your surroundings to prevent security breaches. Be cautious of people following you into secure areas without permission or letting someone into the hall without verifying their identity if they are not expected.
Also, if using a laptop to view or work on village hall related documents, watch out for anyone trying to see your screen or keyboard to steal information (like passwords or PINS).
Always store village hall equipment e.g. SUMUP machine and other devices used for / in the village hall in a secure place when not in use (in the lockable metal cabinet in the storeroom).

PCI-DSS: Handling payment card data and devices
PCI-DSS is a global security standard created to protect payment card data. If you handle payment devices or card data, you must:
• Never write down, store, scan, or transfer village hall payment card data via email, messaging, or social media.
• Delete or securely destroy any card details you come across.
• Only take card details over the phone if authorised and using a PCI-compliant system.

Payment device security
• Log out of devices (SUMUP) when not in use.
• Verify the identity of anyone asking to see your payment devices.
• Do not loan devices without contacting the Treasurer or Secretary
• Keep devices visible during refunds and never leave a device with a customer / resident.
If you think a payment device is stolen or tampered with, don't hesitate to get in touch with the treasurer or secretary who can call SUMUP and Lloyds Bank.

Scams (phishing, vishing, smishing)
Criminals use scams like phishing emails to steal sensitive information, leading to identity theft, financial loss, or data breaches. If you weren't expecting an email, a text, or a call, question it and avoid clicking on any links or interacting with it.

Indicators of a phishing email
• Links asking you to reset passwords or login, or unfamiliar attachments.
• Urgency – emails may pressure you to act quickly.
• Unfamiliar sender or generic greetings—do you know who is contacting you? Even if you do, were you expecting their message? If unsure, verify with the person on a different platform.
Report suspicious emails related to the village hall management to the Secretary or Treasurer