Alderton Village Hall Data Protection Policy and Procedures

REVISION RECORD

Revision Number	Date
1	March 2023

Introduction

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 Alderton Village Hall (AVH). 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 file, and includes email, text messages, social media messages, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, staff and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out the AVH commitment and procedures for protecting personal data. Trustees 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 trustees who collectively decide what personal information AVH 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 Protection Officer – the person responsible for ensuring that AVH follows its data protection policy and complies with the Act. [AVH is not required to appoint a DPO].

Data Subject – the individual whose personal information is being held or processed by [AVH] for example a donor or hirer.

'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him/them.

Explicit consent is needed for processing "sensitive data", which includes:

(a) Racial or ethnic origin of the data subject

(b) Political opinions

(c) Religious beliefs or other beliefs of a similar nature

(d) Trade union membership

(e) Physical or mental health or condition

(f) Sexual orientation

(g) Criminal record

(h) Proceedings for any offence committed or alleged to have been committed

Information Commissioner's Office (ICO) - the ICO is responsible for implementing and overseeing the Data Protection Act 1998.

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 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.

Applying the Data Protection Act within the charity

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, staff and volunteers.

Correcting data

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 must 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.

Responsibilities

AVH is the Data Controller under the Act, and is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for.

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) Collection 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 trustees, 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.

Procedures for Handling Data & Data Security

AVH 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.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA. It is therefore important that all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Privacy Notice and Consent Policy

The privacy notice and consent policy are as follows:

Alderton Village Hall uses personal data for the purposes of managing the hall, its bookings and finances, running and marketing events at the hall, staff employment and its fundraising activities. Data may be retained for up to 7 years for accounts purposes and for longer where required by 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.

The online booking system is configured such that consent must be given by the hirer by ticking the checkbox and agreeing to the following statement before being allowed to continue with making the booking.

Alderton Village Hall uses personal data for the purposes of managing hall bookings, finances, events and publicity. Please tick here to confirm you are willing for us to share your contact details with other groups and organisations benefitting the residents of the Parish of Alderton.

Therefore, a record of bookings made acts as a record of consent by the hirer to these policies.

Operational Guidance

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.

Remember, 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:

• 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.

• If you have any doubts, ask the caller to put their enquiry in writing.

• If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from some- one impersonating someone with a right of access.

Laptops and Portable Devices:

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

Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot.

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.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

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 and preferably contain some numbers. Ideally passwords should be 6 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.

Data Storage:

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. For employee records see below. 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.

Information Regarding Employees or Former Employees:

Information regarding an employee or a former employee, will be kept indefinitely. If something occurs years later it might be necessary to refer back to a job application or other document to check what was disclosed earlier, in order that trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

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 e..g. 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. 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.

APPENDIX A - DEALING WITH A SUBJECT ACCESS REQUEST (SAR)

GDPR strengthens the rights of individuals to obtain confirmation from an organisation as to whether or not personal data concerning them is being used, where and for what purpose. A copy of the personal data has to be provided, free of charge unless the request is 'manifestly unfounded or excessive', in an electronic format, including any emails where they are mentioned. If the data was not obtained from that individual, details of where it came from have to be provided.

This is called a Subject Access Request (SAR). AVH have 30 days in which to respond and certain information must be provided. However, before providing the information, AVH need to verify the individual's identity otherwise we could commit a data breach.

Step 1: Check who we are dealing with.

We could ask questions that only they would know, about reference numbers or appointment details for example. Or we can ask for ID that you can actually verify. ACRE Information sheet 4 suggests both photo identification e.g. passport and confirmation of address e.g. recent utility bill, bank or credit card statement.

Step 2: Check the request is valid.

If the SAR is made by someone other than the person the data is about (such as a friend, relative or solicitor), check they're allowed to have it. You'll need to see that they have written authority to act on behalf of the person concerned, or a document showing general power of attorney.

In most cases, children over 12 are capable of making their own SARs. If you're asked for personal data about a 12-year-old by their parent or carer, you should usually get permission from the child first.

Step 3: Set ourselves some reminders.

We've got one calendar month to get what we need together and send it to the relevant person. If we need to check their ID or ask for other information, we can wait until they reply before starting the clock on our one month time limit, but we should ask for any additional information you need as soon as possible.

There are three important things to know about the one calendar month timeframe:

1. It doesn't matter if the day we receive the request isn't a working day. For example, if we receive a request on Saturday 7 March, we should respond by Tuesday 7 April.
2. If the SAR's due date falls on a weekend or a public holiday, we have until the next working day to respond. For example, if we receive a request on 25 November, we should respond by 27 December.
3. We can't add extra days when the calendar month is shorter. For example, if we receive a request on the 31 January, we should respond by the 28 February.

If it's a very complex request, or if the requester has made a lot of requests, we can take an extra two calendar months to respond, but we must let the requester know there will be a delay before the end of the first calendar month.

Step 4: Check you're on the same page about what they've asked to see.

If we've got the request in writing, read it carefully. It would be easy to assume they're asking for everything we've got, when in fact they've only asked for data relating to one particular thing. They might even be able to give us advice on how to find it. It's okay to ask them. It could save us both some time.

Step 5: Search for the relevant information.

Use the search functions on our smartphone, computer (including archived files), and email folders to find information relating to the person, just as we'd normally do when looking for a particular file. We might need to think creatively about all the places where this information might be held. Depending on how we run our charity, we might need to check external hard-drives, tablets, portable memory sticks, call recordings and social media posts too. Keep looking until you're satisfied there's nowhere else to look.

Step 6: Check what you need to redact.

Before we consider giving the requester their information, look through it carefully to make sure it really is their information.

For example, if we have an email that mentions a number of different people, you should 'redact' (black out) any information which **doesn't** relate to the person making the SAR. This is important, because most of the time we should avoid disclosing information about other people. Another way of doing this is to copy and paste sections relevant to the SAR into a separate document and send them that instead.

Step 7: Consider the impact of releasing data about other people.

Most of the time, we should avoid disclosing information about other people in a SAR. But there may be occasions when the personal data we have pulled together includes information that is closely linked to someone else. In those situations, our aim should still be to release the personal data requested. But we also need to take into account that in doing so we may disclose data about someone else and, at the same time, consider the impact of that.

Step 8: Prepare our reply.

If we got the SAR by email, we should reply by email, unless the requester has said otherwise. Check with them what format they'd like it sent in and give it a final check with steps six and seven in mind.

Step 9: Send our reply securely and keep a record of what you've sent.

As well as the requester's personal data, we need to send our privacy information (a copy of this document). They have a right to know why we hold their data, how we got it, how long we're planning on keeping it, who we share it with, and how they can ask for it to be changed (such as updating their address) or deleted. Make sure we keep dated records of the information we send as we may need to refer to it again, for example if they're unhappy with our response or make another request soon after.

APPENDIX B - DEALING WITH A DATA BREACH

All organisations are required to report certain types of data breach to the Information Commissioner's Office (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.

Step 1: Start the timer.

By law, we've got to report a personal data breach to the ICO without undue delay (if it meets the threshold for reporting) and within 72 hours.

We might end up not needing to report it, but start a log anyway, to record what happened, who is involved and what you're doing about it.

The clock starts from when you discovered the breach, not when it actually happened.

Step 2: Find out what's happened.

Pull the facts together as quickly as possible.

In our log, write down facts about the incident as we uncover them. This could be things like what happened and why, how many people were involved, a timeline of when it all happened, and what actions we've taken so far.

Step 3: Try to contain the breach

Our priority is to establish what has happened to the personal data affected. If we can recover the data, do so immediately. Also, we should do whatever we can to protect those who will be most impacted.

Step 4: Assess the risk

We should now assess what we feel the risk of harm is to those affected, whether that's our customers, members or service users. By risk of harm, consider any potential harm or detriment it may cause to people, eg safeguarding issues, identity theft or significant distress. We might be dealing with a simple mix-up where there's little or no risk involved, or a serious breach that will have a lasting effect on people's lives.

Step 5: If necessary, act to protect those affected.

If possible, we should give specific and clear advice to people on the steps they can take to protect themselves, and what we're willing to do to help them. If we don't think there's a high risk to the people involved, we don't have to let them know about the incident.

Once we've established what happened, tried to contain the breach and assessed the risk of harm to those who have been affected, our next step is to do what you can to protect them further.

There's nothing stopping us telling people about the incident, even if we don't think there's a high risk to them, but we'll want to balance any risk to them against the potential of causing unnecessary worry.

If we think there's a high risk, then by law we have to tell them without undue delay. For example, if we feel there is a high risk of them having their identity stolen, then we have to let them know so they can be extra vigilant and take steps to protect themselves.

Step 6: Submit our report (if needed).

If the breach is reportable, we can call the ICO reporting helpline, on 0303 123 1113, they're open Monday to Friday, 9am to 5pm.

If we're unsure if the breach is reportable, we can use the self-assessment tool on the ICO website to help us decide.

When we report a breach, we'll need to provide details such as what happened and when, our risk assessment, and what we've done to contain the breach. Please be ready to provide as much information as we can, as this will help the ICO give us the most relevant advice for the next steps we should take.