Aberlady Community Association - Aberlady Village Hall

Data Protection Policy

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 to manage Aberlady Village Hall and oversee the governance of Aberlady Community Association (ACA). 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, minutes of meetings, and photographs.

The charity (Aberlady Community Association) will remain the data controller for the information held. The trustees, any future staff and volunteers, whether members or not, are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, any future staff and volunteers, whether members or not, 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 Aberlady Community Association's 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 Aberlady Community Association (ACA) and Aberlady Village Hall 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 ACA follows its data protection policy and complies with the Act. ACA is not required to appoint a DPO and has not done so.

Data Subject – the individual whose personal information is being held or processed by ACA, for example a hirer, ACA member, contractor, Trustee.

'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:

(a) Racial or ethnic origin of the data subject

OSCR
Scottish Charity Regulator
www.oscr.org.uk
Registered SCIO
SC053151

(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 members, volunteers, hirers of Aberlady Village Hall.

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 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 Association, its membership; Hall, its hirings and finances; Newsletter, its distributors. It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to trustees, any future staff and present or past 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

Aberlady Community Association is the Data Controller under the Act, and the Trustees, collectively, are legally responsible for complying with Act, which means that they determine what purposes personal information held will be used for.

The Trustees will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, implement the 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.

OSCR
Scottish Charity Regulator
www.oscr.org.uk
Registered SCIO
SC053151

i) Set out clear procedures for responding to requests for information.

All trustees, any future staff and past and present volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

ACA is not required to appoint a Data Protection Officer. If at some point it chooses to do so then that person will be named here in the policy document. The Trustee responsible for the policy document and reporting to the Trustees is the ACA Secretary.

This policy and associated procedures 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 Data Protection Act 1998. It will be formally reviewed no less than biennially.

Date adopted by the Aberlady Community Association (ACA) Trustees:
01.04.2025……..

Date last reviewed:

Procedures for Handling Data & Data Security

Introduction

Aberlady Community Association (ACA) 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, any future 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 Trustees, staff and volunteers 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 private notice and consent policy are as follows:

Consent forms will be stored by the ACA Secretary in a securely held electronic or paper file.

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 someone 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) and appropriately stored/secured.

Data Security and Storage (Paper Free):

Personal data, as necessary for operational reasons should be stored electronically. Personal data received on disk or memory stick should be saved to the relevant file on a password protected server or laptop. The disk or memory stick should be password secure or encrypted, if not it should be securely returned (if applicable), safely stored or wiped and securely disposed of.

Passwords:

Passwords giving access to personal data should be appropriate, protected and “strong”, containing both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 12 characters or more in length.

Data Storage:

Personal data will be stored securely and will only be accessible to authorised volunteers or Trustees.

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 le isation. All personal data held for the

OSCR
Scottish Charity Regulator
www.oscr.org.uk
Registered SCIO
SC053151

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:

Occasionally it may be necessary 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.

Trustees will 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.