Alfold Hall

Information Security 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 in order to carry on our work of managing Alfold Hall. The 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 include email, minutes of meetings and photographs.

The charity (*Alfold Hall)* will remain the data controller for the information held. The trustees, Committee Members and volunteers are personally responsible for processing and using personal information in accordance with Data Protection Act and GDPR. Trustees, Committee Members 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 Alfold Hall'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 Alfold 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 Alfold Hall follows its data protection policy and complies with the Act. Alfold Hall 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 Alfold Hall, for example a hirer, contractor, Trustee, Committee Member, supporters
- '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:

1. Racial or ethnic origin of the data subject
2. Political opinions
3. Religious beliefs or other beliefs of a similar nature

4. Trade union membership
5. Physical or mental health or condition
6. Sexual orientation
7. Criminal record
8. 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 and GDPR compliance

Processing - means collection, 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 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 UK 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 hiring 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:

Alfold Hall[1] is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

The Committee will take into account legal requirements and ensure that it is properly implemented and will through appropriate management, apply criteria and controls:

1. Collection and use in information fairly.
2. Specify the purpose for which information is used.
3. 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.
4. Ensure the quality of information used.
5. Ensure the right 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, and
4. the right to correct, rectify, block or erase information which is regarded as wrong information.
5. Take appropriate technical and organisational security measures to safeguard personal information.
6. Ensure that personal information is not transferred abroad without suitable safeguards
7. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
8. Set out clear procedures for responding to requests for information.

All trustees, Committee Members and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

At this stage, Alfold Hall has not appointed a Data Protection Officer. If at some point it chooses to do so, then that person will be named here in the policy document.

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 agreed by the Committee: November 2024

Review every two years, or sooner of legislation changes

Information Security Policy V1, 2025

[1] *The Trustees acting collectively*

Procedures for Handling Data and Data Security:

Introduction

Alfold Hall has a duty to ensure that appropriate technical and organisational measurers and training are taken to prevent:

- Unauthorised or unlawful process of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

All Trustees, Committee Members 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 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 private notice and consent policy is as follows:

Consent forms will be stored by the Committee 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 operations 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:

1. 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.
2. If you have any doubts, ask the caller to put their enquiry in writing.
3. 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 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:

As little personal data as possible/ necessary for operational reasons should be stored electronically. 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.

- Password:

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 6 characters or more in length.

- 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 is kept in the kitchen by the first aid box. It 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:

1. Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or any person e.g. child protection,
2. The Data Subject has already made the information public,
3. Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
4. Monitoring for equal opportunities purposes - i.e. race, disability or religion.

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, Committee Members 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.

Registered Charity No: 304963

Information Security Policy: V1.1.25

Date agreed by the Management Committee: Nov 2024, review every 2 years or with any changes to legislation