



Valley Park Community Association

Community Centre, Pilgrims Close, Valley Park, Chandlers Ford,
Hampshire, SO53 4ST

Registered Charity Number: 900526

Tel: 023 8026 6593 Email: centremanager@valleyparkcommunity.co.uk



Data Protection Policy & Procedures

Document Control

File Name	Data Protection Policy & Procedures
Original Author(s)	Isla Thomson, Centre Manager
Current Revision Author(s)	
Owner	Data Protection Officer
Publication Date	March 2021
Review period	Annually or if changes in legislation

Version History

Version	Date	Author(s)	Notes on Revisions
v1	July 2020	Isla Thomson	
v2	March 2021	Isla Thomson	Improved document control and update Data Protection Officer

Document Sign Off

Name	Role	Doc version	Signoff date	Signature*
Kevin Kitcher	Data Protection Officer	v1		
James Crawford	Data Protection Officer	v2		

This is a controlled document. Whilst this document may be printed, the electronic version stored in VPCA Team Resources is the controlled copy. Any printed copies of this document are not controlled.

Acknowledgements

This policy is based on the work of Louise Beaton, a trustee of ACRE, with reference to material published on the ICO website.

Contents

Introduction	3
Purpose	3
Definition of Terms	3
Data Controller	3
Act	4
Data Protection Officer (DPO)	4
Data Subject	4
Explicit consent	4
Information Commissioner's Office (ICO)	4
Processing	4
Personal Information	4
The Data Protection Act	5
Applying the Data Protection Act	5
Correcting Data	5
Responsibilities	6
Data Subject Rights	6
Privacy Notice and Consent Policy	7
Operational Guidance	7
Email	7
Phone Calls	7
Laptops and Portable Devices	8
Data Security and Storage	8
Passwords	8
Data Storage	8
Information Regarding Employees or Former Employees	9
Accident Book	9
Data Subject Access Requests	9
Risk Management	9

Introduction

This policy sets out the application of UK law on data protection regarding how personal information is processed by Valley Park Community Association. Data protection legislation exists to protect individuals from the misuse of personal information including data held in written or computerised formats.

Valley Park Community Association 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 out work in managing Valley Park Community Centre and the Valley Park Voice. This personal information must be collected and handled securely.

The General Data Protection Regulation (GDPR) 2016/679 details key principles, rights and obligations when processing personal data. This applies to the European Union and European Economic Area. The Data Protection Act 2018 (DPA) details the legislative application of the GDPR in the UK.

The Data Protection Act 1998 and General Data Protection Regulations 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 will remain the data controller for the information held unless stated otherwise. 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 Valley Park Community Associations 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 whom we deal with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

Definition of Terms

The following are definitions of the terms used in this policy:

Data Controller

The trustees who collectively decide what personal information Valley Park Community Association will hold and how it will be held or used.

Act

The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) – the legislation that requires responsible behaviour by those using personal information.

Data Protection Officer (DPO)

The person responsible for ensuring that Valley Park Community Association follows its data protection policy and complies with the Act. [Valley Park Community Association is not required to appoint a DPO].

Data Subject

The individual whose personal information is being held or processed by Valley Park Community Association, for example, a donor, hirer, or advertiser.

Explicit consent

Explicit consent is a freely given, specific agreement by a data subject to the processing of personal information about them.

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

- Racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Criminal record
- 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

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 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

We will inform data subjects why we are collecting their data, which is for the purpose of managing Valley Park Community Centre and the Valley Park Voice, including their hiring, advertising, 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 the 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

Valley Park Community Association 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 consider legal requirements and ensure that they are properly implemented; and will through appropriate management, strict application of criteria and controls:

- Collect and use information fairly.
- Specify the purposes for which information is used.
- 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.
- Ensure the quality of information used.
- Ensure the rights of individuals about whom information is held, can be exercised under the Act (See Data Subject Rights).
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation, or ethnicity when dealing with requests for information.
- 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.

Data Subject Rights

- The right to be informed that processing is undertaken.
- The right to access to their personal information.
- The right to restrict processing in certain circumstances.
- The right to correct, rectify, or erase information which is regarded as wrong information.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

The Data Protection Officer on the management committee is:

Name: James Crawford

.....

Contact Details: Email treasurer@valleyparkcommunity.co.uk marked for the attention of the Data Protection Officer

.....

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- Ensuring that everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Ensuring that everyone processing personal information is appropriately trained to do so.
- Ensuring that everyone processing personal information is appropriately supervised.
- Ensuring that anybody wanting to make enquiries about handling personal information knows what to do.
- Dealing promptly and courteously with any enquiries about handling personal information.
- Describing clearly how Valley Park Community Association handles personal information.
- Regular review and audit of the way Valley Park Community Association holds, manages, and uses personal information.
- Regular assessment and evaluation of Valley Park Community Association's 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 Data Protection Act 1998.

In the case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Privacy Notice and Consent Policy

Specific Privacy Notices will be made available on our website and will be reviewed and updated regularly.

Evidence of consent will be stored 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 an individual 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 must 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.

Protecting your password:

- 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 no longer than 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.

An opt-out list will be maintained for those who do not wish to be contacted for marketing purposes in the future. Any marketing lists will be checked against this to ensure no contact is made. VPCA will not make further contact, no contact will be made to check that the removal of consent remains in place.

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:

- Carrying out a legal duty or as authorised by the Secretary of State.
- Protecting vital interest of the data subject or other person e.g. child protection.
- The data subject has already made the information public.
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
- Monitoring for equal opportunities purposes – i.e. race, disability or religion.

Valley Park Community Association 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.

Valley Park Community Association 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 the 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.