Viables Community Association
DATA PROTECTION POLICY

Data Protection Act 1998

The Data Protection Act 1998 took effect on 1 March 2000 and supersedes the Data Protection Act 1984. The Act protects a data subject (any individual on whom data is held) from unlawful processing of data and gives right of access to that data.

Under the new Act, essentially all aspects of handling data qualify as processing. Any data user involved, for example, in the collection, storage, retrieval, alteration, destruction or erasure of data will need to work within the requirements of the Act. In addition, the definition of data is no longer restricted to automatically processed information but also includes manual records.

Viables Community Association needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry out our work. This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this under the new Data Protection Act and General Data Protection Regulation (GDPR) of May 2018. The Data Protection Act 1998 took effect on 1 March 2000, and supersedes the Data Protection Act 1984. The Act protects a data subject (any individual on whom data is held) from unlawful processing of data, and gives right of access to that data.

Scope

The policy applies to all staff, Trustees and volunteers of Viables Community Association.

Data Protection Officer

Viables Community Association is not required to appoint a DPO under the GDPR.

Viables Community Association (VCA) Policy

1. VCA recognises the public's and voluntary/community sector's expectation that their personal information will be handled in accordance with the law.
2. VCA regards the lawful and correct treatment of personal information as important to successful operations and to maintaining the confidence of those people it deals with.
3. VCA fully endorses and will adhere to the eight principles of the Data Protection Act 1998.
    i. The right to be informed
    ii. The right of access
    iii. The right to rectification
    iv. The right to erasure
    v. The right to restrict processing
    vi. The right to data portability
    vii. The right to object
    viii. Rights in relation to automated decision making and profiling.
4. VCA requests that staff and Volunteers familiarise themselves with Operating Guidelines relevant to them and implements them.
5. Breaking data protection law could lead you into prosecution and dismissal.

Disclosure of Personal Information

- **DO** treat personal data with care
- **DO** check identities of people by either asking a question that only a bone-fide caller would know before
  - Disclosing information by phone
  - or ask to see some form of identification before
  - Disclosing information by interview
- **DO** check there is a need-to-know basis before disclosing to colleagues
- **DO** use confidential waste to dispose of documents containing personal data
- **DO** ensure other people cannot see personal data on your computer system or the documents you are using if they have no need to
- **DO** not leave personal data on your desk when you are not there
- **DO** make sure you have adequate secure storage for documents
- **DO** use passwords to protect the data on your computer system and don't share your login and password
- **ONLY** use personal data for the purpose it was collected
- **ONLY** disclose personal data to those people who have a right and a need to know
- **ONLY** disclose personal data to authorised third parties

If You Are In Any Doubt, Don't Disclose, Seek Advice

Security

Staff will check the payment card machine weekly before use to check for signs of tampering.

VCA will ensure that they and any third parties are PCI DSS compliant. We have an Internet, Payment Cards, PCI compliance and Email Policy and take steps to make sure the policy is implemented.

The Roger Morris Community Centre has internal CCTV and the association ensure there is appropriate signage to inform users of that. The association will follow the Surveillance Camera Code of Practice and has registered with the ICO (Information Commissioner's Office.) All CCTV footage is deleted once 30 days have lapsed and is only used and reviewed for the purpose of ensuring safety and security of the building, its facilities, our staff/volunteers and users.

Asking for consent

We have checked that consent is the most appropriate lawful basis for processing some of our data. See Appendix A for more detail.

- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.

Managing Consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.

- We make it easy for individuals to withdraw their consent at any time and publicise how to do so.
- We will comply with requests for erasure, rectification or restriction by individuals of/to personal data
- We act on withdrawals of consent as soon as we can.
- We don't penalise individuals who wish to withdraw consent.

Data Breach

If any of our team detect a data breach, we will document it and contact our IT consultant as well as the Chairman (and the ICO if necessary) to ensure we assess the likely risk to an individual as a result;

For data breaches that pose a high risk to an individual, we will notify the ICO (Information Commissioner's Office) of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

We inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

For all requests by Individuals, Viables Community Association aims to respond as quickly as possible, and within one month.

Third Party Processing

For Office 365 storage (email/files), Viables Community Association stores data in line with Privacy Policy of Microsoft.

- **Transfer of Customer Data**. Unless Customer has opted out of the Standard Contractual Clauses, all transfers of Customer Data out of the European Union, European Economic Area, and Switzerland shall be governed by the Standard Contractual Clauses. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland.

  Extract taken from Microsoft Volume Licensing Online Services Terms (Worldwide English, November 2016)

- The booking system used by Viables Community Association – Planyo - uses Amazon AWS for file storage and this service is compliant with the EU Model Contract Clauses.

- Trybooking – this is used to book activities and events. Their privacy policy can be found here.
  - https://www.trybooking.com/uk/info/privacy

- Opayo – online payments – their Privacy Policy can be found here.

- https://developer-eu.elavon.com/docs/opayo-forms/compliance/pci-compliance

Monitoring and Review

The Senior Management Team, with adequate consultation of the Board of Trustees, will regularly review the operation of this policy.

Agreed by VIABLES COMMUNITY ASSOCIATION	
Signature: B. Hibbert	Date: Feb 2023