Internet, Payments Cards, PCI and Email Policy
FOR THE VIABLES COMMUNITY ASSOCIATION

The protection of the Association's reputation, intellectual assets and the information it holds about living individuals (personal data) is a critical responsibility for all employees and volunteers. Violation of this Policy could lead to legal and/or disciplinary action.

SCOPE

This Policy applies to all Viables Community Association employees and volunteers for the use of the Association's Visa, E-mail and Internet facilities.

Use of these facilities is password controlled. The passwords are not stored within the office and are given out only to those employees and volunteers who have been approved by the Committee. Passwords are alpha numeric, at least 8 characters long. The same password must not be used for multiple systems and will be changed when prompted or when there is a staff change.

The facilities comprise PCs, laptops, a PDQ Classic Visa terminal and an Office 365 tenant (viables.org.uk). A network diagram detailing office-based equipment for Viables Community Centre is provided in Appendix A for the purpose of securing the network related to our card reader for PCI DSS Compliance

Bruce Hibbert is the Management Trustee currently responsible for security issues.

E-MAIL USAGE

1. E-mail is provided for use in the effective delivery of the Association's Services.

2. E-mails should be kept as brief as possible and the subject line of the message should always provide a clear description of the message contents.

3. Users should be selective when forwarding or replying to an E-mail and consider who really needs to see the message – forwarding it only to those who need the information.

4. Users should first consider whether alternative means of communication would be more appropriate (e.g. a telephone call or face to face discussion).

5. Users should delete E-mail messages once read, provided they do not need to refer back to them for the purpose of the work being undertaken. Only messages that really need to be kept should be saved. Any attachments that need to be kept should be extracted and filed in the proper folder.

6. Users should check E-mail regularly on each working day.

7. Users must always disclose their identity and declare their relationship with the Viables Community Association when using E-mail by using their electronic signature.

8. Private use of the E-mail facilities should be kept to a minimum and only for essential purposes.

9. Misuse of the Association’s E-mail service and E-mail forgery is a violation of this Policy. Examples include:

- Sending offensive, abusive or libellous messages.
- Intentional impersonation and/or misrepresentation.
- Modifying a message and forwarding it without highlighting the changes.
- Fabricating a message.
- Bypassing user security systems in a malicious manner (e.g. creating bogus accounts).
- Forwarding the Association’s sensitive information or personal data to external sources.
- Originating or participating in E-mail chain letters.
- Knowingly burdening the E-mail systems with non-business critical data (e.g. large amounts of personal communications).

DISCLAIMER

All E-mails will automatically contain the following disclaimer:

This electronic communication (and any attachment) is intended for the above named only. It may contain private/confidential information. If it has come to you in error, please take no action based upon it and neither read it or copy it, nor cause its contents to be disclosed to others. If you realise an error has been made (or we notify you of an error) please completely delete/destroy all electronic/hard copies and telephone us (at our expense) to let us know this has been done.
Colin is this up to date?

This disclaimer will be attached by Microsoft Outlook as a ‘signature’ when an E-mail is sent using the Association’s internet service.

INTERNET USAGE

1. Access to the Internet including the World Wide Web (“Web”) is provided for use in the effective delivery of the Association’s services.2. Misuse of the Association’s Internet service is a violation of this Policy. Examples of misuse include:

- Intentionally accessing or transmitting material which is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts
- Knowingly doing anything which is illegal under English law or the law of any other relevant country
- On-line Gambling

3. Software must not be downloaded from the Internet (to protect from viruses and copyright infringement). All downloads of software will be discussed with our paid IT consultant in any instance.

4. The Association reserves the right to:

- Withdraw users’ access to any computer systems and communication services, including Internet services.

- Prohibit access to certain web pages and other Internet resources.

CARDHOLDER DATA

1. The Association will store only the data elements needed for business. The full magnetic stripe data [name; primary account number (PAN); expiration date; card validation code] will not be stored.

2. The full card number will not be used unless operationally essential. We will not store card holders' PAN. The card number will be concealed wherever possible.

3. The card validation code will not be stored.

4. The personal identification number (PIN) will not be stored.

5. The PAN will be masked when displayed.

6. No PANs or other details will leave the premises, be entered into messaging technologies such as email, or copied onto removable media such as CDs and memory sticks.

7. Access to cardholder data will be limited to those individuals whose jobs require such access.

8. Paper that contains cardholder data will be classified as confidential and physically secure.

9. All hardcopy materials containing cardholder data will be classified as confidential. It will be destroyed when it is no longer needed for business or legal reasons by cross-cut shredding, so that cardholder data cannot be reconstructed.

10. Access to the card machine is limited to those trained to use it and to visually inspect for tampering only.

PCI DSS Compliance

The 12 requirements of PCI DSS are:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

12. Maintain a policy that addresses information security for all personnel

    VCA will

    - complete annual compliance checks with their card reader company (currently Barclaycard).
    - Pay an IT consultant to manage and maintain the systems and networks that provide security and access, including checking for open ports where the network is segmented.
    - Not retain card data beyond putting payments through the machine. Please see above at Cardholder Data for full details.
    - Use Barclaycard provided Sysnet Protect software to run scans that check the security of our systems – though card details are not kept anyway.

SECURITY INCIDENT RESPONSE

1. The Committee is responsible for establishing and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.

2. All security incidents should be reported immediately to the Centre Manager and Chair for investigation.

LEGISLATIVE REQUIREMENTS

1. Please refer to our Data Protection Policy for details.

RESPONSIBILITIES

1. You have a responsibility to ensure that you comply with the Association's Internet, Payment Cards , and E-mail Policy.

2. Adherence to the Policy is a condition for using the Association's equipment. Failure to comply with this Policy may result in legal claims against you and the Association or lead to disciplinary action being taken.

3. The Management Committee is responsible for ensuring that the Internet, Payment Cards , and E-mail Policy is implemented.

GENERAL REQUIREMENTS

1. All computers should be locked or switched off when not in use.

2. All portable PCs and any portable equipment must be locked away when not in use.

3. Introducing a virus can lead to the infection severely affecting computer systems and data. All electronic storage devices must be virus checked prior to use and only VCA purchased storage devices must be used.

4. Carry out weekly tamper inspections to the card machine – ensure that the serial no. is correct and that the machine has no signs of physical tampering.

Date reviewed: Feb 2023

Date of next review: Feb 2024