# Information and Communication Technology Security Policy

## 1. Introduction

CVS Cheshire East (CVS) recognises the importance that all of its systems are protected to an adequate level from vulnerabilities.

Such risks include accidental data change or release, malicious damage (internal or external), fraud, theft, failure and natural disaster.

It is important that a consistent approach is adopted to safeguard CVS's information in the same way that other more tangible assets are secured, with due regard to the highly sensitive nature of some information held on both electronic and manual systems.

## 2. Purpose

As well as a common law duty of care, CVS has a legal obligation to maintain security and confidentiality for the data it holds, including: the GDPR and Data Protection Act 2018.

It is the duty of CVS and its staff and volunteers to meet these legislative and regulatory requirements in relation to Information and Communication Technology (ICT) Security.

This policy sets out the procedures to be followed by all staff and volunteers to ensure that CVS's ICT assets — hardware, software and data — are protected.

It is aimed at ensuring:

- Confidentiality: data access is confined to those with specified authority to view the data
- Integrity: all systems are working as they were intended to work and all data protected from unauthorised change
- Availability: data is available to the right person, when needed

## 3. The need for a Security Policy

Data stored in information systems represent an extremely valuable asset. The increasing reliance of CVS on ICT for the delivery its services makes it necessary to ensure these systems are developed, operated, used and maintained in a safe and secure fashion.

The increasing need to hold personal data for contracting and service delivery and transmit this information across ICT systems managed by CVS renders data more vulnerable to accident or deliberate unauthorised modification or disclosure. The use of computers to exchange data electronically offers advantages to CVS members if handled securely, but could present serious hazards if security is inadequate.

## 4. Scope

This policy applies to all CVS staff (both permanent and non-permanent), volunteers and contractors or staff employed by other organisations but working on behalf of the organisation. It also applies to all areas of CVS's 'business' so covers all Information Assets, be they member related, or not.

CVS has made a firm commitment to monitor and protect its confidential information. This may be person identifiable information relating to members or staff members or it may be documents of a commercially confidential or sensitive nature.

It has, therefore, become a fundamental principle of CVS to have an effective and consistent ICT Security Procedure in place.

## 5. Duties and responsibilities

The Chief Executive has responsibility for all elements of data protection and security of information. Matters of exception are reported to the Board of Trustees who have oversight for this.

The Chief Executive is supported by the Management team whose duties in relation to ICT Security include:

- Periodically report to the Board of Trustees, through the Finance and Compliance Committee the state of ICT security
- To keep up to date with new developments and requirements to ensure the ICT security policy remains current
- Ensure that ICT security policy is implemented
- Ensure compliance with relevant legislation including GDRP,
- Help ensure that all staff are aware of their security responsibilities by assisting with regular ICT security awareness training and providing support and guidance for all users
- Assist with Internal Audit plans to review CVS's compliance with any external contractual security policies
- Recommend software / hardware purchases in the organisation.

All staff and volunteers are responsible for ensuring that they comply with CVS's information security requirements, including ensuring they apply the standards set within the ICT Security policy.

## 6. Procedures

CVS will maintain an inventory of the physical assets associated with its information systems; this will include:

### Physical Assets

Each physical asset will be assigned an "owner". The owner of all physical assets (computer hardware and associated peripheral equipment) is CVS but for practical purposes (security marking, inventory, maintenance etc.) this is delegated to the Finance and HR Manager / Third Party IT Support Company.

### Software Application Assets

The Finance and HR manager will also be responsible for maintaining a register of all software applications deployed, including ensuring CVS holds copies (or evidence) of relevant licences.

### Access Control

A key element of ICT Security is ensuring suitable controls are in place to restrict access to those who actually need it. Also, it is important to ensure that measures are in place to prevent misuse or theft of the relevant assets.

### CVS Systems

The Chief Executive is responsible for the leading on security for all the CVS-wide electronic systems, including the maintenance and developments of related procedures and policies. Special attention will be given to the allocation of "privileged" or "supervisor" rights, which will normally be available only to certain members of the management team on a 'need to know' basis.

## Gaining access

To access to any 'Information Asset' the user must first have an authorised and active CVS user account, which will be approved by the line manager/Chief Executive

- Access to the CIVRM Database will be approved and actioned by the line manager or Chief Executive
- Access to the Sharepoint Office 365 System will be approved by the line manager and will be actioned by the third party IT provider.
- Access to Xero (Financial management software) will be approved by the Chief Executive and actioned by the third party provider
- Access to SAS-Protect (HR management software) will be approved by the line manager and actioned by the Finance and HR manager

Levels of access will be set by the Chief Executive and will be maintained by the Finance and HR Manager, they will be responsible for:

- keeping a record of all users for each system
- remove the access rights of any staff who have changed jobs or left the organisation
- periodically checking for and removing redundant accounts that are no longer required
- ensuring all users' access rights will be reviewed periodically to ensure that access levels remain consistent with their duties.

In gaining access for users the staff member approving will:

- check that the level of access requested is consistent with organisational security policies (See Appendix 1)

## Password management

All ICT systems will have an automatic password reset function and no lists of password for staff or volunteers will be stored on the system.

In setting passwords and communicating these to new staff members or sending reminders no single email will contain both the username and password.

All systems used by CVS which hold personal data will have an individual username and password to access the system. There will be no group accounts. This is to ensure that there is accountability and transparency in the use of the system and limit the potential for accidental disclosure of passwords.

Passwords will:

- be complex and contain at least 7 characters with, at least one upper case letter, one number and one symbol.
- Allow users to select and change their own password and include a confirmation process to check for spelling errors
- Enforce a password change every 3 months
- Not display password on the screen while typing
- Limit the number of incorrect logins to 3 with the account being locked out and administrator being contacted
- timeout to log users out when not at their computer

All new staff should be briefed on the importance of passwords and instructed in the manner in which they are to be used and protected as part of the staff induction process.

Access to computer services and data will be controlled on the basis of business requirements and is the responsibility of the Chief Executive in cooperation with the data "owner" and relevant managers.

## 7. Equipment Security

CVS is a cloud based organisation and so does not manage or maintain and servers or business critical equipment on its sites. Staff and volunteers are required to use a laptop/computer in fulfilling their role which is provided by CVS.

The Finance and HR Manager will ensure that:

- all CVS PCs and laptops are installed with virus protection software,

- CVS discourages the use of USB or data transportation and only CVS approved USB memory keys are permitted read/write access data containing personal or sensitive information. These keys are encrypted on first use. Unencrypted memory keys will only have read access

- Any critical equipment is protected from power failures through use of uninterruptible power supplies (UPS). These systems will warn of electrical failures and automatically initiate orderly shutdown if power is not restored within a specified time

- any maintenance arrangements that are the subject of contractual agreement have only approved system engineers accessing

- each individual laptop/computer has an individual secure login with a password to access the PC.

- each individual laptop/computer has an administration account to enable access this password is not available to staff and is held by the third party ICT company.

CVS contracts with a third party IT provider to support with the security of the ICT systems this includes the individual computing devices.

It is the policy of CVS that staff and volunteers are not authorised to store any data on the hard drives of their computers as there is no back up function. All data is stored on the Office 365 system which is secured with a 30 day back up.

## 8. Disposal of ICT equipment

When a laptop/desktop computer becomes obsolete or is broken beyond repair then all data is removed from the hard drive including the operating system. The hardware will then be disposed of through appropriate methods.

## 9. System Planning, Procurement and Acceptance

Acquisition of any new ICT asset must conform to all standards set out within this policy.

All systems holding personal data will be hosted within the EEA and will meet all requirements laid out by the GDRP, DPA 2018 and Information Commissioners Office

All security requirements should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

- Major applications etc will be considered by the Management team and consulted with final approval from the finance and compliance committee.
- Minor applications will be considered and approved by the Management Team.

In the acquisition of new hardware or systems the management team must consider:

- how hardware or software changes which may affect network management are agreed by all parties affected.
- any new ICT facilities provide an adequate level of security and will not adversely affect existing security
- mandatory, as defined above, and desirable security requirements are included in procurement specifications
- Access controls and User Management, appropriate to the purpose and content of the new asset, should be included in the procurement specification.
- Suitable back-up and disaster recovery procedures will be in place
- Training requirements are considered for any new hardware and software involved in the new asset, both for local management and IM&T support
- set documented user acceptance criteria against which the system can be tested.

### Physical security measures to be taken by all users

When in use, mobile devices should never be left unattended, especially when working off-site. Make use of room locks and lockable storage facilities where available.

- Where the mobile device must be left for a few hours or overnight it should be logged off and stored in a locked drawer or cabinet.
- All removable media such as CD-ROM and USB keys should be disabled or removed unless absolutely necessary.
- When travelling and not in use, ensure that mobile devices are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the boot. Mobile devices left on display and unattended will inevitably attract attention and are likely to be stolen.
- Do not leave mobile devices unattended in car boots overnight.
- When travelling, avoid placing mobile devices in locations where they could be easily forgotten or left behind e.g. overhead racks and taxi boots.
- Be aware that the use of mobile devices in public places is likely to draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.
- Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc and on public transport e.g. buses and trains.
- It is good practice to carry mobile devices in protective anonymous bags or cases (i.e. those without manufacturer logos on them) when not in use

## 10. Training Requirements

These procedures reinforce many of the requirements set out in policies such as GDPR policy, Data Breach Policy and Data retention policy.

All staff will receive awareness training on this policy and related ICT security polices listed above. Staff will also receive training in any specific systems they will use as part of their role which will reinforce any security requirements.

## Appendix A – Access levels in Systems

| Name of System | Level of access | Typical role with level of access |
|---|---|---|
| CIVI CRM database and website | Super Admin | RedHot Irons (third party supplier) and 2 Staff members, Chief Executive and Marketing Manager |
| | Full, add, delete Edit of Database and Website | All Staff member |
| | Limited, add or edit of website or database | Volunteers |
| | Basic login edit their individual data | Volunteers applying for roles |
| | Basic login only edit their data and access data of volunteers applying | Volunteering Organisations |
| Office 365 Sharepoint | Admin rights | Axon (third party supplier full Admin rights)<br>Chief Executive Admin rights |
| | Able to access all files and documents held | Chief Executive and Finance HR Manager |
| | Restricted access (e.g. not able to access HR documents) | All staff and volunteers |
| | Access to shared emails and calendars e.g. enquiries@cvsce.org.uk | Staff members |
| Xero (Financial package) | Full access to system | Shires accountants (third party supplier) and Chief Executive |
| | Full editing and reporting rights | Chief Executive and Finance HR Manager |
| | Rights to view information, no editing | Management team |
| SAS Protect (HR Package) | Full access to the system (ability to change policies etc) | SAS Daniels (third party supplier) |
| | Admin rights to the system | Chief Executive and Finance HR Manager |
| | Line management rights, approve holiday etc. Restricted view to staff that are managed | Management Team |
| | Restricted access only access and edit their data | All staff members |