Volunteer Cornwall
Information Security Policy

Introduction

This information security policy shall apply to information, systems, networks, applications, locations, staff, volunteers, and trustees of Volunteer Cornwall.

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by Volunteer Cornwall. This shall be achieved by:

- Ensuring that all members of Volunteer Cornwall staff and volunteers are aware of and shall comply with the General Data Protection Regulation (GDPR).
- Describing the principles of information security management and describing how they shall be implemented within Volunteer Cornwall.
- Introducing an approach to information security that is consistent with other organisations.
- Assisting staff and volunteers to identify and implement information security as an integral part of their day-to-day role within the practice.
- Safeguarding information relating to staff and clients under the control of Volunteer Cornwall.

Objectives

Key objectives of this Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to those staff and volunteers of Volunteer Cornwall and relevant others with agreed authority to view it.
- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered when it is needed.

Responsibilities for Information Security

- Responsibility for information security shall rest with the Chief Executive. However, on a day-to-day basis the Accounts and Administration Manager shall be responsible for organising, implementing, and managing this policy and its related good working practices.
- Senior Managers shall be responsible for ensuring that both permanent and temporary staff including volunteers and contractors are aware of:
  - The information security policies applicable to their work areas
  - Their personal responsibilities for information security
  - Who to ask or approach for further advice on information security matters.
- All staff, volunteers and trustees shall abide by security procedures of Volunteer Cornwall. This shall include the maintenance of client records whilst ensuring that their confidentiality and integrity are not breached. ***Failure to do so may result in disciplinary action.***
- This Information Security Policy document shall be owned, maintained, reviewed, and updated by the Accounts and Administration Manager. This review shall take place annually. The results of which shall be made known to the Chief Executive and the Board of Directors.
- Staff and volunteers of Volunteer Cornwall shall be responsible for both the security of their immediate working environments and for security of information systems they use (e.g., workstations, laptops, PDAs etc.).
- Any contracts with third party organisations that allow access to the information systems of Volunteer Cornwall shall be in place before access is allowed. These contracts shall ensure that

the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by Volunteer Cornwall.

Volunteer Cornwall shall undertake to ensure:

Contracts of Employment – address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.

Access Controls - to areas containing information systems are restricted and controlled to ensure that only those authorised can access information.

Equipment Security – is effective to minimise losses, or damage to Volunteer Cornwall. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked cabinets (fireproof if possible), clear desk policy and the limitation of risks in the surrounding work area etc).

Information Risk Assessment – a regular assessment of the working environment shall be conducted to identify potential risks to the security of Volunteer Cornwall's information. Where risks are identified, these should be noted and where possible mitigating action taken.

Security Incidents and weaknesses - are to be recorded and reported to the Chief Executive so that they can be investigated to establish their cause, impact and the effect on Volunteer Cornwall and its clients and stakeholders. (NB. remedial changes arising may need to be included within future staff working procedures, updates to policies and contracts of employment).

Protection from Malicious Software – should be provided using commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of Volunteer Cornwall without the explicit permission of the IT Officer. Breach of this requirement may be subject to disciplinary action.

Secure Communications – should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of client records are conducted in a secure and confidential manner. The communication of Confidential or restricted information by email must be appropriately protected.

Business Continuity and Disaster Recovery Plans – are in place so that in the event of a disruption to the information services of Volunteer Cornwall, it is possible to activate relevant business contingency plans until affected services are restored.

Signed:  Date

Ian Jones

Chief Executive

On behalf of Volunteer Cornwall Review Date: 04/25