Volunteer Cornwall
Monitoring & Audit Policy

Introduction

Information and information systems are important assets, and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of Volunteer Cornwall.

The aim of this policy is to maintain the quality, confidentiality, and availability of information stored, processed, and communicated by and within Volunteer Cornwall. These policies, standards, guidelines are used as part of the data security and protection management system within Volunteer Cornwall.

Volunteer Cornwall places great reliance upon the robust application of the policies and standards that make up its Data Security and Protection policy and has, therefore, developed processes to self-assess compliance.

This policy applies to all staff and volunteers, whether permanent, part-time, or temporary with responsibilities defined below.

Responsibilities Within This Policy

All employees and volunteers have responsibilities regarding this policy.

Monitoring

Context

Auditing, by its nature, is based on samples and random checks and, while providing valuable assurances to the Board, it does not take away the responsibility to self-manage, ensuring compliance with its Data Security and Protection policy as well as legal and regulatory requirements.

To this end Volunteer Cornwall reserves the right to monitor the activity of individuals in appropriate circumstances acknowledging the legal requirements and restraints applicable.

In determining the need for and appropriateness of monitoring due reference has been made to the Information Commissioner's Monitoring at Work Guidance, The Human Rights Act, and the Regulation of Investigatory Powers Act.

In particular, the Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training).
- In the interests of national security.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ensuring the effective operation of the system.

In addition, communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of Volunteer Cornwall's business, and the employee's position with Volunteer Cornwall.

Impact Assessment

Having due regard to the sensitivities related to client and other information and the need to demonstrate to the public our determined efforts to ensure effective information governance it is the opinion of Volunteer

Cornwall that it is appropriate that it retains the right to monitor information flows within as well as into and out of Volunteer Cornwall.

Volunteer Cornwall is aware that monitoring is a sensitive issue, and it seeks to minimise any adverse impacts through effective consultation and communication with staff.

Examples of monitoring

While not intended to be exhaustive or all inclusive, the list below provides examples of the monitoring which Volunteer Cornwall does or may wish to undertake: -

- Examining logs of web sites visited to ensure appropriateness.
- Using internet filtering software to block and report on inappropriate internet access attempts.
- Scanning of e-mail for inappropriate content.
- Randomly opening e-mails or listening to voicemails for evidence of inappropriate practice.
- Monitoring of telephone logs for evidence of inappropriate contacts e.g., premium rate numbers.

While several of the above, e.g., internet logs, internet filtering and e-mail scanning, may be routinely in place others may be invoked as and when a concern of needs arises.

Internal Audit

Policy Statement

It is the policy of Volunteer Cornwall that all aspects of its Data Security and Protection will be subject to an internal review at least once every 12 months. This will help ensure that not only policies and procedures are being applied but that new best practice can be gathered and applied.

Process

Overview

This audit process is undertaken by Volunteer Cornwall senior managers and is distinct to audit work undertaken by its auditors. It is undertaken in discussion with staff members in the area under review, identifying whether existing procedures are complied with and at the same time identifying whether the procedures are adequate. This will involve observing work in progress as well as sampling previous records. The senior manager (auditor) will also gauge overall security awareness of the staff members interviewed.

Internal Audit, Monitoring and Compliance Checklists are at Appendix A and should be completed annually by individual senior managers.

Audit Checklists will be used for guidance only and will not limit the enquiries of an auditor who is following the audit trail. In addition, the Audit Checklists may be used to record relevant information during the audit.

Reporting Audit Findings

Findings will be recorded and subsequently will be classified by the auditor, as either a recommendation or as an observation. This will be recorded on an audit summary form at Appendix B).

The Auditor will ensure that each recommendation has a unique identification number (the audit number followed by a second sequential number). This information will be added to the Internal Audit log. The respective manager will sign to accept the recommendation.

At the end of the audit the Auditor will generate an Audit Report at Appendix C. This Report will consist of any Audit Checklists and notes, copies of any observations, copies of any recommendations, if applicable, a summary of the audit findings and a front page. The front page will detail the Area/Function audited, the unique audit number, the date and time the audit was carried out, the auditor(s), auditee(s) and a list of attachments.

An urgent 'Recommendation' indicates that an aspect of Data Security and Protection is either not defined or not being adhered to in any way and hence a risk to the business. Such a recommendation would need to be addressed as a matter of urgency.

The auditor may also see fit to raise an 'Observation' which is not a firm recommendation but rather a suggestion for improvement. Upon the next visit, the auditor will expect the 'observation' to have been taken on board (if appropriate) thus signifying ongoing improvement to Data Security and Protection. Any non-site-specific observations will be shared with other sites.

Following Up Corrective Actions

Once the Chief Executive has received the completed non-conformities the Audit Summary Form is then updated to show when a follow up review is required. The purpose of this verification (follow up) audit is to ensure that the defined corrective actions have been successfully implemented and are effective. The auditor who raised the original recommendation normally conducts this audit.

Once objective evidence has been found confirming the successful implementation and effectiveness of the actions, the recommendation will be closed and signed off by the auditor and the department representative. The Chief Executive and Information Governance lead will review the recommendation and authorise its closure.

Breaches of Confidentiality

Actual, potential or near misses of confidentiality should be reported using Volunteer Cornwall's Information Security Incident Management and Reporting Procedures.

Compliance

Responsibility

It is the responsibility of all users to ensure that they have read, understood, and abide by this standard.

Signed: 

Date

Ian Jones
On behalf of Volunteer Cornwall

Due Review: 04/25

APPENDIX A

Volunteer Cornwall
Data Security and Protection Monitoring, Compliance, Spot-checks and Internal Audit Checklists and Report

Department/Activity/Project:

Audit carried out by:

Date:

PART ONE: DATA SECURITY AND PROTECTION CONFIDENTIALITY INTERNAL AUDIT

Section: ICT Security	**Detail**	**Actions or Recommendations**
How many PCs within the area?		
How many PCs are within a public area?		
How many are secured against theft?		
How are they secured against inappropriate access?		
Check if any logged in and left unattended - observation		
Are screens viewable by the public or visitors?		
Are all PCs linked to the network?		
Random check of C drives for confidential information - observation		
Random check of keyboards, diaries, draws etc. to find passwords written down - observation		
Is the equipment security marked?		
Is the equipment protected against malicious software or code?		
Is virus software up to date?		
Section: Communications		
Where are the main calls routed through?		
Is this the main reception area?		
Is there a facility for calls to be taken in privacy?		
Check to see if calls can be heard from public areas – observation		
Is there an answer machine in public areas?		
Is this listened to whilst the public are present?		
Section: Physical Security		
Is access to staff only areas restricted by a security device?		
Are there any areas that are closed for lunch?		
Are these areas secured against entry during these periods?		
Are there window locks on downstairs windows?		
Is there a burglar alarm?		
Are there environmental controls to prevent flooding, environmental issues?		

Section: Security of Confidential Information		
Is confidential information used in public areas? What security is used to protect this information?		
Are locked cabinets available?		
Check the area, walls, and desks to see if confidential information is clearly on view – observation		
Within work areas is confidential information kept secure?		
Can confidential information be seen from outside of work areas?		
Any other observations?		
Section: Records Security		
How are records stored?		
How often are records archived?		
Where are archived records stored?		
How long are records kept?		
Section: Disposal of Confidential Information		
How is confidential information disposed off?		
How regularly is it disposed off?		
Section: Training Requirements		
Training identified as a result of the internal audit		

PART TWO: DATA QUALITY CHECKLIST

Criteria	Yes	No	Actions or Recommendations
Do you know the sources of all the data you hold?			
Is there a system for regular updating of all personal and contact data stored?			
Do people know who you are and what you are doing with their data?			
Do you need to get their consent for anything? If so, how will you do that?			
Is the data stored as securely as possible with all reasonable back-up and password protections enabled?			
Do you have adequate security for information that is taken out of the office?			
Do your staff and volunteers know what they are supposed to do with personal data, and what they are not allowed to do? Are they aware of their responsibilities?			
Is all the personal data held within the organisation monitored and subject to the same security and updating procedures?			
Is the holding of each type of personal data fully justified as furthering the aims and legitimate work of the Centre?			
Is the data you hold still necessary for the purposes for which it was originally collected?			
Is the data kept up to date?			
Does the information held on individuals threaten their security in any way?			
Does the personal data include any speculation?			
Does all the information come from reliable sources and are all sources noted?			
Do you keep records of why, with whom and when the data is used?			
Random (10%) sample of records checked to confirm Accuracy, Reliability, Timeliness, Relevance, Completeness and Compliance.			
Error/Omission Logs checked, and corrective action taken.			
Are all staff entering data effectively trained?			

PART THREE: DATA SECURITY AND PROTECTION COMPLIANCE CHECKLIST

Volunteer Cornwall

Data Security and Protection Compliance Checklist

Audit Undertaken by:	
Date of Audit:	

Routine Staff Monitoring & Compliance Spot Checks	
Confirmed that the Data Security and Protection (DSP) Policy has been made available to all members of staff and volunteers.	☐
Confirmed that staff members know where to find the DSP Policy and the purpose of the policy.	☐

Contract Clauses	
Confirmed that the list of staff, temps, volunteers, contractors and third parties with access to personal information is up to date and complete.	☐
Confirmed that staff members know where to find the DSP Policy and the purpose of the policy.	☐

Data Security and Protection Training	
Confirmed that all new starters have received training on Data Security and Protection as part of their induction.	☐
Confirmed that all staff including temporary, volunteer and contract staff have completed or are in the process of completing basic DSP training, and that the basic DSP training is sufficient.	☐
Evidence that training needs are regularly reviewed and re-evaluated where necessary.	☐
Confirmed that staff in key roles have received additional DSP training as necessary.	☐
Confirmed that staff understand their key responsibilities (e.g., checked that staff understand the confidentiality code of conduct).	☐

Shared Information	
All purposes that require confidential information to be used or shared has been clearly identified and have a documented and lawful basis. All staff supporting these purposes understand what is lawful and what is not.	☐
All data breaches have been correctly reported, or there are no breaches.	☐

Client Awareness	
Leaflets about the use of personal data are available to clients, and available in different formats to meet the needs of service users with special or different needs.	☐
Staff members can answer detailed questions service users may have about the use of their information or know who to refer the service user to.	☐
	☐

Staff Understanding of Confidentiality Code of Conduct	
Confirmed that staff members know where to find the confidentiality code of conduct and the purpose of the Code.	☐
Confirmed that staff members know who the Information Governance Lead is and who to contact for support on Data Security and Protection issues.	☐
Confirmed that staff know their own responsibilities for compliance with the code.	☐
Confirmed that staff members know that client information should not normally be shared without consent.	☐
Confirmed that staff working off-site or at home know not to remove client identifiable information from Volunteer Cornwall.	☐

Staff Understanding of Procedure for New Processes	
Confirmed that staff members know where to find the procedure for ensuring that information security, confidentiality and data protection, and information quality requirements are considered before new changes to processes, services or systems are introduced.	☐
Confirmed that staff members know that they need to seek approval before introducing changes to processes, services, or systems and how they should seek approval.	☐
Confirmed that relevant staff know how and when an appropriate Privacy Impact Assessment should be carried out.	☐
Confirmed that Data Protection Impact Assessment documentation is available for review.	☐

Staff Understanding of Confidentiality and Audit Procedures	
Confirmed that appropriate staff members understand their responsibilities for monitoring and auditing access to confidential personal information.	☐
Confirmed that appropriate staff members understand that monitoring and audit is being carried out, of the need for compliance with confidentiality and security procedures and the sanctions for failure to comply.	☐
Confirmed that where a breach has occurred, copies of incident reports etc. are available for review.	☐
Confirmed that where a near-miss has occurred, copies of incident reports etc. are available for review.	☐

Asset Register	
Confirmed that staff members understand the need for an Asset Register and who is responsible for the register.	☐
Confirmed that a documented Information Asset Register is maintained and up to date.	☐

Review of compliance with Mobile Computing Guidelines	
Confirmed that staff are aware of the confidentiality and security risks associated with using mobile computing equipment, and that they have been issued with relevant guidelines.	☐
Anti-virus and back-ups recently updated.	☐
Confirmed that access to internal systems is controlled and that robust authentication procedures are in place for all staff having remote access to systems.	☐
The record of issue and ownership of mobile devices is maintained and up to date.	☐

Business Continuity	
Confirmed that there is a documented up to date Business Impact Analysis.	☐
Confirmed that there is a documented up to date Business Continuity Plan.	☐
Confirmed that staff are aware of the Business Continuity Plan and any implications for their role.	☐

Incident Management and Reporting Procedure	
Confirmed that staff members know who to report suspicious incidents to and what their own responsibilities are with regard to incident reporting.	☐
Confirmed that staff know where the Incident Management and Reporting Procedures can be located for managing different types of incident and near-misses.	☐
Completed incident reporting forms and reports are available for review.	☐

Compliance with Access Controls	
There is a documented procedure for allocating and managing access to computer-based information systems.	☐
Confirmed that only staff regularly working at Volunteer Cornwall are authorized users and have active user profiles and have access rights appropriate to their role.	☐
Confirmed that all staff are aware of their responsibility to appropriately access and use the system. There is no evidence of staff not following procedures, e.g. using somebody else's password and username.	☐
Where users have left or no longer require access to the system, confirmed that their rights have been revoked.	☐

Compliance with Secure Transfer Procedures	
Confirmed that there is a documented procedure for the secure transfer and receipt of personal and sensitive information.	☐
Are staff members who transfer and receive personal information aware of the appropriate methods for secure transfer and receipt of personal information. Are client records being stored securely when not in use?	☐
Is the security of password(s) to access the system being maintained (i.e. passwords not written down and left beside the computer)	☐
Is waste which includes personal information being put into the secure shredding bags or shredded?	☐
Do staff members ensure that sensitive conversations with clients are not overheard?	☐

Review of compliance with Data Transfer Procedures	
Are envelopes containing personal information being marked 'private & Confidential'?	☐
Confirmed that personal information is secure when being sent.	☐
When providing information over the telephone is the callers identify always confirmed?	☐
Confirmed that staff members are not copying any personal information to unencrypted memory sticks?	☐

Compliance with Network Security	
Confirmed that there is a documented Network Security Policy for each ICT Network.	☐
Reviews of information security risk in relation to ICT networks are undertaken and documented with full details of controls and procedures put in place to mitigate any risks identified.	☐
Confirmed that staff have been informed of and understand their responsibilities regarding network security.	☐

Accuracy of Service User Information	
Confirmed that documented procedures are in place incorporating all aspects of data collection, validation and correction of errors, and that these are available to all staff.	☐
Confirmed that staff have received relevant training and know what action to take when errors or omissions are identified.	☐
Confirmed that regular checks between clients records and actual data held on systems have been carried out and errors or omissions have been corrected.	☐
Data quality reports are held.	☐

Part Three Actions or Recommendations:

APPENDIX B

PART FOUR: SUMMARY OF AUDIT ACTIONS FORM

Department:

Manager:

Date:

Finding/Observation/Detail	Normal/Urgent	Actions or Recommendations	Completed, Implemented or Closed date
PART ONE:			
PART TWO:			
PART THREE:			

Certified that all actions and recommendations have been completed or implemented or will be by the date shown above.

Signed: Date:

Name:

APPENDIX C

PART FIVE: Data Security and Protection Monitoring, Audit, Compliance and Data Quality Report

IG Lead: Lisa Crook

To: IG Steering Group and SMT

Subject: Data Security and Protection Monitoring, Audit, Compliance and Data Quality Report

1. **Scope and Objective**

The audit undertaken aimed to assess Volunteer Cornwall's compliance with its internal Data Security and Protection System.

This particular review focused on the following elements of information governance;

- Confidentiality;
- Data Quality;
- Information Governance Compliance.

2. **Summary of Findings / Observations**

The audit identified xx non-conformances of which xx were considered to be of an urgent nature. These findings are summarised below:-

FINDING	ACTION/RECOMMENDATION

In addition, there were xx observation raised which are summarised below:-

FINDING	ACTION/RECOMMENDATION

3. **Conclusion / Opinion**

Having assessed the findings arising from the review it is apparent that the Data Security and Protection policy *has / has not (delete)* been consistently applied.