Volunteer Cornwall
Data Security and Protection 2024

Information, Communications, Telecommunications and Technology

Contents:

Information, Communications, Telecommunications and Technology Policy

Telecommunications
Regulations setting out the circumstances in which businesses can record and monitor e-mails and telephone calls came into force on 24 October 2000. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provide for several circumstances in which it will be lawful for Volunteer Cornwall to intercept, monitor and record communications without the consent of sender, recipient, or caller. In short, these include the following purposes:

- To establish facts relevant to Volunteer Cornwall's business, e.g., where most transactions are done by telephone.
- Ensuring compliance with regulatory or self-regulatory rules or guidance.
- Gaining routine access to business communications, e.g., if an employee is absent.
- Maintaining the effective operation of their systems, e.g., to check for potential viruses.
- Monitoring standards of service and training.
- To investigate or detect unauthorised use of a system, e.g., inappropriate e-mails or downloading unsuitable materials from the Internet.

In addition, monitoring, but not recording, without consent is available for the purposes of determining whether the communications are relevant to the business.

A lawful interception is one that is made either with the consent of the parties, or "in the course of lawful business practice", when consent is not needed. If Volunteer Cornwall wishes to use the powers contained in the regulations to monitor or record without an employee's consent, then Volunteer Cornwall must make all reasonable efforts to inform every person who may use the system that communications may be intercepted.

The new regulations come under the Regulation of Investigatory Powers Act 2000 (RIP Act) which establishes a new legal framework to govern the interception of communications during their transmission on public or private telecommunications systems. It also establishes a basic principle that communications may not be recorded or monitored without the consent of the senders or recipients. The purpose of the Lawful Business Practice Regulations is to make sure that legitimate business practices are not prevented by the new regime.

Internet and E-Mail Guidance
The Volunteer Cornwall Internet and E-mail operating guidance is attached to this policy.

Security of Data
Information is only to be input or accessed by authorised users, as approved by senior managers. Users are to ensure the accuracy of information entered.

Senior managers are to ensure that all IT systems under their control are password protected, with a copy of the password held by the IT Officer. Users are to change their passwords in accordance with the Volunteer Cornwall guidelines on the appropriate use of computer systems.

No sensitive or personal data is to be transferred electronically unless its security can be guaranteed. The Information Technology Officer is to ensure that appropriate software is in place to safeguard all transmitted data.

No unencrypted laptops, drives, memory sticks or other portable data containing personal data are to be taken out of office premises. This also applies to those removable portable devices or media which can store personal data, and be connected to a computer, such as memory drives, memory sticks and pens, removable hard drives, as well as CDs and DVDs etc. It will also include devices such as PDAs or smartphones where they have been used to store or process personal data. Where a laptop or other removable portable devices are not encrypted, then they must not be taken out of the office if it contains personal data.

Unauthorised software or shareware is not to be loaded onto Volunteer Cornwall computers.

Back-Up Procedure
A dedicated information back-up procedure is to be in place for all Volunteer Cornwall's IT systems. The minimum requirement is that 3 back-ups are in use, and it is recommended that 1 back-up is taken out of the building, 1 back-up is kept in a different building and 1 back-up is kept in a fireproof container. Senior managers are responsible for ensuring that appropriate back-up procedures are in place for their departments.

Anti-Virus Software
All Volunteer Cornwall's IT systems are to have anti-virus software installed. The Information Technology Officer is to ensure that appropriate anti-virus software is in place to safeguard all systems. It is staff responsibility to upgrade virus alert systems.

If material is inadvertently accessed which is believed to contain a computer virus, a user is to immediately break the connection, stop using the computer and contact the Information Technology Officer for assistance.

Verification of Data Held
Senior managers are to ensure that all data held electronically is accurate, up to date and essential for Volunteer Cornwall to store. It is recommended that, at the most, annual reviews of data held should be formally carried out.

Training
Senior managers are to ensure that IT training requirements are reviewed as part of the appraisal process.

Signed: Date:
Chief Executive Due Review: 04/25
Volunteer Cornwall

OPERATING GUIDANCE FOR THE USE OF ELECTRONIC COMMUNICATIONS

General

All staff and volunteers now use a variety of electronic communications in their day-to-day work. Staff and volunteers within Volunteer Cornwall now have access a wealth of information on the Internet. This information has the capability to enhance both the quality and effectiveness of our services.

In acknowledging the many benefits that the Internet, for example, will bring to our work, we must also be aware of the inherent risks associated with being connected to such an information and communication system. These risks include:

- Computer viruses
- Access to offensive material, for example material containing racist terminology, nudity, bad language, or violence.
- Access to pornographic material
- Security of information
- Confidentiality of information
- Abuse of E-mail
- Employer's liability regarding material sent through e-mail.

This policy applies equally to the use of social networking sites such as Facebook or X formally Twitter on Volunteer Cornwall matters.

Aim

The aim of this policy is to enable Volunteer Cornwall and its employees comply with the Data Protection Act regarding electronic communications and the adoption of good practice.

Use of Telephone Systems (Including Mobile Phones)

Volunteer Cornwall's general policy on the use of telephone systems is that they are only to be used for business use. However, there are occasions when staff need to make personal calls during working hours to discuss personal matters with organisations such as banks, dentists, doctors etc. In these circumstances, and with the senior manager's approval, staff may make short (15 minutes or less) telephone calls from their work landline.

Company mobile phones are **not** to be used for personal use. In accordance with current legislation mobile phones are **not** to be used when driving on Volunteer Cornwall business.

On no account are overseas or premium rate calls to be made from company landlines or mobile phones.

Internet and E-mail Safeguards

- Volunteer Cornwall's general policy on the use of the internet and e-mail facilities is that they are only to be used for business purposes. However, it is appreciated that there are occasions when staff need to access the Internet for personal use. In these circumstances, and with the senior manager's approval, staff may access the Internet for personal use for no longer than 30 minutes at a time, provided it does not interfere with the business of the office and takes place outside normal working hours.

- Files are not to be downloaded from the Internet unless they have a specific business need. The loading or running of unlicensed software is forbidden and copyright must be respected when downloading or forwarding information from the Internet. This also applies to e-mail attachments.

- **E-mail must not be opened unless it is known to have been received from a recognised source**. If there is any doubt about the originator of the e-mail it is **not** to be opened, and advice should be sought from the IT Officer.

- All users are not to view or download offensive or distressing material such as material containing racist terminology, nudity, bad language, or violence.

- All users are to ensure that colleagues are not unwittingly exposed to material that could cause offence or distress.

- Users are not to send material via e-mail that could be considered, by the receiver or inadvertently by anyone viewing the e-mail, as offensive or distressing.

- The content of e-mails should not breach the Volunteer Cornwall's equal opportunities and other policies.

- Under no circumstances are users to access, receive or distribute pornographic material. This will be considered as **gross misconduct**.

- Identifiable personal information or otherwise sensitive data should not, under normal circumstances, be sent over the Internet or by e-mail.

- Users are to ensure that any material they send, retrieve, or receive complies with local policies, directives and laws pertaining to data protection, confidentiality, and copyright.

- All users should note that during any absence or annual leave, their emails may need to be accessed for various reasons. A senior manager will make a request to the IT Officer who will log onto the specific users account and go through the information with the senior manager before logging out of the account.

It is also extremely important to be aware that sending e-mail via the Internet can, in certain circumstances, lead to litigation against the employer. An employer may be held liable if defamatory, sexist, or racial messages or other offensive material are sent by e-mail. Advice given on e-mail has the same legal bearing as any other written advice.

Copyright Infringement

The main risk of copyright infringement is attached to downloading files from the Internet. Copyright infringement can also occur where text is copied into or attached to an e-mail message.

Equally, users must not transmit copyright software from their computer to the Internet or permit anyone else to access it on their computer via the Internet. Users should not copy information originated by others and re-post it without permission from, or at least acknowledgement of, the original source, even if the content is modified to some extent.

Copyright and other rights in all messages posted to the Internet from an employee, like other material produced at work, belongs to Volunteer Cornwall, and not to users personally.

Users are not to assume that information posted on the Internet originates from the person or organisation who appears to have produced it, without some form of authentication.

Breach of the Safeguards
Users are to report any inadvertent breaches of these safeguards immediately to the Accounts and Administration Manager.

Breach of these safeguards may result in disciplinary action and in serious cases could lead to **immediate dismissal**. Volunteer Cornwall may deal with violations of the above policies by any combination of:

- Verbal warning.
- Denial of Internet access for a period.
- Denial of Internet access permanently.
- Disciplinary action, potentially for gross misconduct, through the normal disciplinary process.
- Provision of information to the police for possible criminal proceedings.

The Chief Executive will **actively** monitor all aspects of Internet access and the e-mail usage of members of staff. This will be done by a variety of methods including spot-checks and audit of Internet and e-mail logs and will include any sites visited, duration of access and e-mails sent and received.

Blogging and Social networking
Online diaries, or blogs, have become increasingly popular as sources of information. Social networks such as Facebook and X formally Twitter have also become increasingly popular as a means for people to stay in touch and make new contacts.

Although these are personal accounts there is some concern that staff could spend a lot of time on these sites whilst at work. There is also the concern that work issues could be discussed on these sites.

It is therefore important that there are clear guidelines over the use of these sites by staff. If staff wish to access these sites they may, with the senior manager's approval, access the site for personal use for no longer than 30 minutes at a time, provided it does not interfere with the business of the office and takes place outside normal working hours, e.g., lunchtime.

Confidential work matters are not to be discussed on these sites and any defamatory statements made on these sites about Volunteer Cornwall or its staff will be treated as disciplinary offences.

Disclaimers
Disclaimers and notices are to be used in conjunction with existing internal controls. All published web pages are to have a disclaimer or a link to a separate disclaimer page.

Confirmation of Receipt of Operating Guidance
There are serious implications to both staff and Volunteer Cornwall if the safeguards detailed in this policy document are not followed. All staff are therefore requested to return the attached reply note confirming that they have received, read and understood the contents of this policy statement.

Volunteer Cornwall's Policy for The Use of Electronic Communications
Confirmation of Receipt of Operating Guidance

To: IT Officer

I, ……. (print name)

Have received a copy of Volunteer Cornwall's Policy for The Use of Electronic Communications, which I have read and understood.

I am aware that any breach of the Policy may result in Volunteer Cornwall's disciplinary procedures being invoked. The disciplinary procedure may, under certain circumstances, lead to immediate dismissal.

Signed: ……. Date: ……

Annex B

GUIDELINES ON THE APPROPRIATE USE OF COMPUTER SYSTEMS

These guidelines apply to all staff and volunteers including permanent and temporary members of staff.

Personal use of IT equipment
IT facilities such as the Internet and email have been provided by Volunteer Cornwall primarily for business purposes. Volunteer Cornwall permits the personal use of these facilities (normally limited to lunch breaks and after work hours) with senior manager permission.

Excessive personal use or inappropriate use of the IT systems is a disciplinary offence and may lead to dismissal.

- Excessive personal use includes carrying on a business using Volunteer Cornwall's email and other IT facilities.
- Inappropriate use includes accessing or downloading pornographic or offensive images and material, or sending harassing or offensive emails.

Appropriate use of email
Junk/Spam emails and chain letters sent via email should be marked as junk if a user receives one, this will allow the mail spam filters to better identify junk mail over time. Users should not keep this type of mail or forward any to other users.

- Never reply to a junk email even if there is a link to unsubscribe. If you do reply, it can confirm that your email address is valid and will result in you receiving even more junk mail.
- You are expected to manage your email in a professional manner. Email at work is primarily provided for work purposes. In Volunteer Cornwall, staff may use the system for personal mail provided it is not excessive and with the senior managers permission.

Audit trails and reporting security breaches
Nearly all activities you perform on a computer can be tracked. The system enables review and monitoring of internet usage, emails, phone calls and other such usage. Recorded information will be used to aid an investigation where breaches of security, the law or these guidelines are suspected. This information is kept confidential, but when used helps to explain innocent situations more often than exposing security breaches.

Information security breaches might involve unauthorised use of equipment or unauthorised access to data. Any breach of security, however small, wastes time and often requires work to be repeated and could be a potential risk to Volunteer Cornwall or individuals. If you know or suspect that a breach of information security has occurred, please inform your senior manager or information governance lead.

Unlicensed software and computer viruses

You should never install or use software that hasn't been authorised by the IT Officer on your work computer. The main reasons why you should never do this are:

- The risk of infection to your computer, other computers and the network from malicious code embedded in the software. The risk applies to all programmes and games downloaded from the Internet, on CD or any other storage media. Malicious code includes computer viruses, spyware and malware, and the effects will vary depending on which has been downloaded. Some malicious code will just waste time while another can destroy data or even allow a malicious user to gain access to your computer.
- The likelihood of breaching copyright and licensing laws. Volunteer Cornwall must pay for a licence for the software used on its systems. If you install software without authorisation this process is by-passed, and you put Volunteer Cornwall at risk of legal action from the owner of the software. If you are installing so-called free software, it could be an illegal copy, or it could be trial software with an expiry date. Even if neither of these things apply, the software is likely to be for single personal use and require a licence for corporate use.
- The download may interfere with management or other software causing them to run more slowly or not work at all.

If you find some software you think Volunteer Cornwall could benefit from, please inform your senior manager and/or the IT Officer, and NEVER install it yourself!

Malicious code can be contained within any files downloaded from the internet. Volunteer Cornwall has anti-virus systems in place that will catch most incoming viruses, but always be cautious when downloading files from unregulated sites and of email attachments from people you don't know.

Preventing unauthorised system access

Whenever you leave your desktop computer unattended, get into the habit of locking it so that information cannot be accessed by unauthorised persons. To quickly lock your computer, press Ctrl, Alt and Delete then select "lock computer", this will then require password authentication before regaining access to the system. When leaving your workstation for the day, log out of the system entirely and close down the computer.

Password management

For good password management:

- Use at least 6 alphanumeric characters, a mixture of upper and lower case and ideally add some special characters (e.g. $, £, ?, *, _) to further increase security;
- Choose a password that cannot be guessed and avoid using the names of children, partners, pets, your car registration number, or football team etc.
- Use phrases to help you make a complex and more secure password. For instance, 'One day I will visit the US' can become 'o-d-i-w-v-t-u-s' by using the first letter of each word. Then change some of the letters for numbers or special characters, for example, change the letter o to a zero, change the letter i to a forward slash, etc.
- Change your password regularly or immediately if you suspect someone has gained unauthorised access to your account.
- Never share your passwords with anyone, not even your closest colleague. If you suspect someone may know it, change it immediately.

Remember:

- Always keep your password secret.
- Never keep your password written down unless securely locked away.
- Always ensure no one is watching as you enter your password.
- Never share a password and never ever attempt to gain access to a system using someone else's password.

Annex C

Guidelines for the use of Portable Computer Devices, Mobile Phones and Removable Media

Introduction
Volunteer Cornwall recognises that the use of portable computer devices and removable media which help staff in the performance of their duties is becoming more widespread. This guidance aims to support staff who use these devices by ensuring they are aware of information and security issues.

Definitions:

Portable Computer Devices – this includes laptops, notebooks, tablet computers, PDA's (personal digital assistants) and mobile phones.

Removable Data Storage Media – this includes any physical item that can be used to store and/ or move information and requires another device to access it. For example, CD, DVD, tape, or digital storage devices (flash memory cards, USB disc keys, and portable hard drives). Essentially anything you can copy, save and/or write data to which can then be taken away and restored on another computer.

Scope
This guidance applies to all Volunteer Cornwall staff including temporary staff and volunteers.

Only authorised staff should have access to portable computer devices and removable data storage media.

Any member of staff allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action.

Users should also be aware of the home working and Remote Access guidelines.

Use of Portable Computer Devices

DO …
- Complete an asset control form (see Appendix A) for portable devices received.
- Store portable equipment securely when not in use, both on and off site
- Store portable equipment securely when not in use off site
- Security mark portable equipment with a company security tag or other such security method, e.g., UV pen.
- Install a BIOS password, if necessary and where possible
- Secure hard drives or system partitions with password protected encryption software or other

security method to prevent data access should the device be lost or stolen.

- Ensure that portable computer devices are configured to lock (requiring a password to resume), after a maximum period of 5 minutes inactivity.
- Use and regularly update Anti-virus & Firewall (Internet Security) software.
- Be aware of data stored on mobile devices and back up as required.
- Ensure a nominated person is responsible for each portable equipment.
- Maintain a register where portable equipment is recorded to enable identification of current user.
- Obtain authorisation prior to the removal of portable equipment from the premises.
- Be aware that software and any data files created by staff on Volunteer Cornwall portable computer devices are the property of Volunteer Cornwall
- Report **immediately** any stolen portable equipment to the police and senior manager (failure to report a stolen mobile device could result in significant charges)
- Be aware that the security of your portable computer device is your responsibility, and you should check your home and car insurance policies to ensure they cover for business use.
- Ensure that when portable devices are required to be disposed of / re-issued the disposal procedures in Appendix B are followed.
- Ensure that portable devices are returned to Volunteer Cornwall if you are leaving employment.

DO NOT …

- Use your own portable computer device or removable data storage media for Volunteer Cornwall business unless authorised by a senior manager.
- Leave portable computer equipment in places where it can easily be stolen.
- Leave portable computer equipment visible in the car when traveling between locations.
- Leave portable computer equipment in an unattended car.
- Leave portable computer equipment unattended in a public place.
- Install software or download software / data from the internet, unless specifically needed for your role within Volunteer Cornwall
- Disable the anti-virus or firewall protection software.
- Use portable computer devices outside Volunteer Cornwall premises without authorisation.
- Allow unauthorised personnel/friends/relatives to use allocated equipment.
- Delay in reporting lost or stolen equipment,
- Attach unauthorised equipment to the network.
- Remove person identifiable information off site without authorisation from your Senior Manager

Appendix A:

Portable Equipment - Asset control

Asset Control
This is an auditable record of portable equipment currently on the **Volunteer Cornwall assets register.**
Short description of asset: …….. Asset number: …… Mobile Number …… Date entered register: …….. Indelibly marked to indicate property of Volunteer Cornwall: YES / NO
Allocated to: (Named person)……. Located at: ……..
DECLARATION **I (print)……. agreed and understood the User Procedures and the Use of Portable Computer Devices, Mobile Phones & Removable Media Guidelines.** **I understand that it is my responsibility to report <u>immediately</u> any theft, loss, damage or misuse of the above asset.**

Failure to do so could incur disciplinary action or financial penalties.

Signed: …….. Dated: ……..

Appendix B – Disposal / Re-issue of Volunteer Cornwall Owned Portable Computer Devices & Removable Data Storage Media

When an item requires disposal or is no longer required i.e., a person is leaving employment then the following procedures should be followed:

Portable Computer Devices:

These items can be re-issued within Volunteer Cornwall, but the asset register must be updated accordingly, and any sensitive / confidential information removed. If the item is no longer required, then it should be disposed of correctly and a 'Disposal of Portable Asset' form should be completed- see Appendix C. (Please do not send items through the post).

Removable Data Storage Media:

These items should be re-used or destroyed locally. If the items contain sensitive or confidential information this must be removed before re-issue or if requiring disposal, they should be shredded / incinerated accordingly.

Appendix C: Disposal of Portable Asset

DISPOSAL OF PORTABLE ASSET FROM REGISTER
This is an auditable record of portable equipment to be <u>removed</u> from **Volunteer Cornwall:** **…… assets register.**
Short description of asset: …….. Asset number: …… Date entered register: ……..... Date removed from register ……. Indelibly marked to indicate property of Volunteer Cornwall: YES / NO
Removal Process Information: …… ……
DECLARATION The above asset has been removed from the asset register and has been disposed of in accordance with Volunteer Cornwall procedures **Signed: …….. Print Name:……..** **Dated: ……**

Annex D

Remote and Home Working Policy and Procedures

Aim of the Policy

To manage and prevent unacceptable risks arising to Volunteer Cornwall and other information assets by using unapproved or unsafe remote or home working facilities.

Scope

All staff who are permitted to use Volunteer Cornwall equipment remotely or at home, or who may use their personal computing resources to connect to the Volunteer Cornwall network infrastructure are subject to the requirements of this IG policy and procedure. These staff will be required to have read through this document and to sign the agreement declaration Appendix A.

Responsibilities

The IT Officer is responsible for the local definition of network, infrastructure, and PC information security requirements and for the supply and configuration of all computing equipment provided by the organisation. This will include network connectivity and support for approved services.

In exceptional circumstances, remote/home workers may be required to use their personal computing resources for business purpose. The IT Officer must be satisfied that the resources concerned are configured appropriately and security measures are implemented to ensure that no unacceptable information governance risks exist.

The IT Officer is responsible for conducting remote/home risk assessment surveys where necessary and for the identification of any necessary improvements or controls that affect the proposed remote/homework area. In addition, the IT Officer will provide guidance to the remote/home worker on all relevant security policies and responsibilities.

A remote/home risk assessment survey will be necessary when an individual who regularly works remotely or from home, (defined as at least 6 times during a year), has access to:

- Documents protectively marked as ‘confidential’ or above.
- other commercially or otherwise sensitive documents.
- any sensitive person identifiable information about clients or staff.
- person identifiable information about clients or staff deemed non sensitive but still significant in terms of quantity (defined as 50+ records)
- anonymised information about clients or staff.

Unless instructed otherwise, the home worker is responsible for ensuring that their home contents insurance cover extends to all provided equipment belonging to the Volunteer Cornwall.

Data Security Procedures for Remote/Home Working:

The remote/home worker’s proposed working environment(s) should be considered and where necessary surveyed, and any perceived IG risks assessed. The findings of this survey process and any associated risks should be documented, so that appropriate control measures may be reviewed.

Where the proposed remote/home working arrangements involve the use of personal or shared computing resources, it must be noted the IG risks of doing so may outweigh any operational advantage of remote/home working. For all remote/home working scenarios, consideration of risks must be made and should take account of the potential to:

- accidentally breach client confidentiality.
- disclose other sensitive data of Volunteer Cornwall to unauthorised individuals.
- loss or damage critical business data.
- damage Volunteer Cornwall's infrastructure and e-services through spread of un-trapped malicious code such as viruses.
- create a hacking opportunity through an unauthorised internet access point.
- misuse data through uncontrolled use of removable data storage media such as USB flash drives and other media.
- cause other operational or reputational damage.

When a remote/home working agreement is possible the purpose, terms and conditions should be formally reviewed and agreed by the remote/home worker. A reference copy of this agreement must be provided to the remote/home worker. All such remote/home working agreements should be reviewed periodically for their continued applicability.

Steps should then be taken to define, agree and implement the environmental security controls deemed necessary. The IT Officer should maintain records of all such assessments, surveys, related decisions, agreements, and implementation plans.

It is the responsibility of the remote/home worker to maintain their remote/home working environment in conformance with Volunteer Cornwall's policies and agreement permitting their remote/home working. Where a remote/home worker requires clarification or guidance they should consult the IT Officer.

The remote/home worker should be made fully aware of their information governance responsibilities to Volunteer Cornwall. Training should be provided for any additional or special tools or functions that underpin the security of their remote/home working, including provided access and log-on tokens. Such facilities and the training in their use are the responsibility of IT Officer. This may for example include guidance on the deletion of cached information from internet browsers used to access web-based services.

Failure by staff to observe and maintain their remote/home working agreement may result in their remote/home working facility being withdrawn.

It is the responsibility of IT Officer to ensure that Volunteer Cornwall's infrastructure is maintained in a technically secure manner that would reasonably prevent a security breach arising from a remote/home worker's location.

Once all necessary steps have been satisfied the remote/home working arrangements agreed may be made operational. Please note that other IG codes of practice and good practice guidance for information governance security management, the use of data encryption tools and for the security of permitted removable media remain applicable and should be followed.

Audit spot checks should be considered by Volunteer Cornwall to ensure this remote/home working policy is complied with and the agreement with the remote/home worker should clearly specify that this may occur. Any compliance issues will be reported to the senior managers concerned and may be handled through staff disciplinary processes or contractual arrangements.

All incidents involving the use of remote/home working facilities must be reported to Volunteer Cornwall's IT Officer immediately and in accordance with the organisation's incident reporting procedures.

Appendix A

Volunteer Cornwall's Policy for Remote and Home Working
Declaration of Compliance with the Policy

To: IT Officer

I, …… (print name)

Have read, understood, and will comply with Volunteer Cornwall's Policy for Remote and Home Working.

I am aware that any breach of the Policy may result in Volunteer Cornwall's disciplinary procedures being invoked. The disciplinary procedure may, under certain circumstances, lead to immediate dismissal.

Signed: ……. Date: ……

Network Security Policy

Introduction

This document defines the ICT Network Security Policy for Volunteer Cornwall. The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

1. Aim

The aim of this policy is to ensure the security of Volunteer Cornwall's network. To do this Volunteer Cornwall will:

- Ensure Availability
- Preserve Integrity
- Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets.
- Preserve Confidentiality
- Protect assets against unauthorised disclosure.

2. Network definition

The network is a collection of communication equipment to allow access between devices such as servers, computers, printers, and routers, which have been connected by physical cable or by WiFi or other wireless connections. The network is created to share data, software, peripherals, internet connections, hard disks, and other data storage equipment.

3. Scope of this Policy

This policy applies to all networks within Volunteer Cornwall used for:

- The storage, sharing and transmission of data.
- Printing or scanning data.
- The provision of Internet systems for receiving, sending, and storing data

4. The Policy

The overall Network Security Policy for Volunteer Cornwall is described below:
The Volunteer Cornwall information network will be available when needed, can be accessed only by legitimate users, and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality. To satisfy this, Volunteer Cornwall will undertake the following:

- Protect all hardware, software, and information assets under its control.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost-effective manner.
- Will comply with all laws & legislation as appropriate and where relevant - including:
    - Copyright, Designs & Patents Act 1988
    - Access to Health Records Act 1990
    - Computer Misuse Act 1990
    - The Data Protection Act 1998
    - The Human Rights Act 1998

- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Ensure the policy has been approved by the Chief Executive and Board of Directors.

5. Risk Assessment

- Volunteer Cornwall will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity, and availability.
- Risk assessment will be conducted to determine the levels required for security barriers that protect the network.
- Formal risk assessments will be conducted and reported to the Board of Directors.

6. Physical & Environmental Security

- Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity, and power supply quality.
- Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
- Critical or sensitive network equipment will be protected from power supply failures.
- Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating, and drinking is forbidden in areas housing critical or sensitive network equipment.
- All visitors to the secure network areas must be authorised by the IT Officer.
- All visitors to the secure network areas must be made aware of network security requirements.

7. Access Control to the Network

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to Volunteer Cornwall's Remote Access Policy.
- Senior managers and the IT Officer must approve user access.
- Security privileges, network permissions and access to resources will be allocated on the requirements of the user's job, rather than on a status basis.
- All users on the network will have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret (see User Responsibilities).
- User access rights will be immediately removed or reviewed for those users who have left Volunteer Cornwall or changed jobs.

8. Third Party Access Control to the Network

- Third party access to the network will be based on a formal contract that satisfies all necessary security conditions.
- All third-party access to the network must be logged.

9. External Network Connections

- Ensure that all connections to external networks and systems have documented and approved System Security Policies.
- Ensure that all connections to external networks and systems conform to the System Security Policies.
- The IT Officer must approve all connections to external networks and systems before they commence operation.

10. Maintenance Contracts

- The IT Officer will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Information Governance Asset register.

11. Data and Software Exchange

- Formal agreements for the exchange of data and software between organisations must be established and approved by the IT Officer.

12. Data Backup and Restoration

- The IT Officer is responsible for ensuring that backup copies of network configuration data are taken regularly.
- Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all relevant staff.
- All backup tapes will be stored securely, and a copy will be stored off-site.
- Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
- Users are responsible for the security of their own data - ensuring it is backed up or stored in a suitable location on the network where it will be backed up overnight as part of the regular company data daily backup.

13. User Responsibilities, Awareness & Training

- Volunteer Cornwall will ensure that all users of the network are provided with the necessary security guidance, awareness, and where appropriate training to ensure their security responsibilities are met.
- Irresponsible or improper actions by users may result in disciplinary action(s).

14. Accreditation of Network Systems

- Ensure that the network is approved by the IT Officer before it commences operation. In this role the IT Officer is responsible for ensuring that the network does not pose an unacceptable security risk to the organisation.

15. Security Audits

- The IT Officer will require checks on, or an audit of, actual implementations based on approved security policies.

16. Malicious Software

- Ensure that measures are in place to detect and protect the network from viruses and other malicious software.

17. Secure Disposal or Re-use of Equipment

- Ensure that where equipment is being disposed of the IT Officer must ensure that all data on the equipment (e.g. on hard discs or tapes) is securely overwritten. Where this is not possible the IT Officer should physically destroy the disc or tape.
- Ensure that where discs are to be removed from the premises for repair, where possible, the data is securely overwritten or the equipment de-gaussed by the IT Officer.

18. System Change Control

- Ensure that the IT Officer reviews changes to the security of the network. All such changes must be reviewed and approved by the IT Officer. The IT Officer is responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.
- The IT Officer is responsible for ensuring that selected hardware or software meets agreed security standards.
- As part of acceptance testing of all new network systems, the IT Officer will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.

19. Security Monitoring

- Ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

20. Reporting Security Incidents & Weaknesses

- All potential security breaches must be investigated and reported to the IT Officer. Security incidents and weaknesses must be reported in accordance with the requirements of the organisation's incident reporting procedure.

21. System Configuration Management

- Ensure that there is an effective configuration management system for the network.

22. Business Continuity & Disaster Recovery Plans

- Ensure that business continuity plans and disaster recovery plans are produced for the network.
- The plans must be reviewed by the IT Officer and tested on a regular basis.

23. Unattended Equipment and Clear Screen

- Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.
- Volunteer Cornwall operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked when left unattended for a short time.
- Users failing to comply will be subject to disciplinary action.

24. Security Responsibilities

- The Chief Executive has delegated the overall security responsibility for security, policy and implementation to the IT Officer and Accounts and Administration Manager.
- Responsibility for implementing this policy within the context of IT systems development and use in the organisation is delegated further to the IT Officer.

25. IT Officer's Responsibilities

- Acting as a central point of contact on information security within the organisation, for both staff and external organisations.
- Implementing an effective framework for the management of security.
- Assisting in the formulation of Information Security Policy and related policies.
- Advise on the content and implementation of the Information Security Programme.
- Produce organisational standards, procedures, and guidance on Information Security matters for approval by the Information Governance Steering Group.
- Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on information security matters, including representing the organisation on cross-community committees.
- Ensuring that appropriate Data Protection Act notifications are maintained for information stored on the network.
- Dealing with enquires, from any source, in relation to the Data Protection Act and facilitating Subject Access Requests.
- Advising users of information systems, applications, and networks of their responsibilities under the Data Protection Act, including Subject Access.
- Advising the Information Governance Lead on breaches of the Act and recommended actions.
- Encouraging, monitoring, and checking compliance with the Data Protection Act.
- Liaising with external organisations regarding Data Protection Act matters.
- Promoting awareness and providing guidance and advice related to the Data Protection Act as it applies within Volunteer Cornwall.
- Creating, maintaining, giving guidance on, and overseeing the implementation of IT Security.
- Representing the organisation on internal and external committees that relate to IT security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
- Ensuring the systems, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally.
- Ensuring that access to the organisation's network is limited to those who have the necessary authority and clearance.
- Providing advice and guidance to development teams to ensure that the policy is complied with.
- Approving system security policies for the infrastructure and common services.
- Approving tested systems and agreeing rollout plans.
- Advising on the accreditation of IT systems, applications, and networks.
- Providing a central point of contact on IT security issues.
- Providing advice and guidance on:
    - Policy Compliance
    - Incident Investigation
    - IT Security Awareness
    - IT Security Training
    - IT Systems Accreditation
    - Security of External Service Provision
    - Contingency Planning for IT systems

- Contacting the Information Governance Lead when:
    - Incidents or alerts have been reported that may affect the organisation's systems, applications, or networks.
    - Proposals have been made to connect the organisation's systems, applications or networks to systems, applications or networks that are operated by external organisations.
    - Passing on the advice of external sources/authorities on IT security matters.

26. Senior Manager's Responsibilities

- Ensuring the security of the network, that is information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Ensuring that their staff are made aware of their security responsibilities.
- Ensuring that their staff have had suitable security training.

27. General Responsibilities

All personnel or agents acting for the organisation have a duty to:

- Safeguard hardware, software, and information in their care.
- Prevent the introduction of malicious software on the organisation's IT systems.
- Report on any suspected or actual breaches in security.

28. Validity of this Policy

This policy should be reviewed annually by the Board of Directors, under the authority of the Chief Executive. Associated information security standards should be subject to an ongoing development and review programme.

Allocating and Managing Access to Computer/IT Systems Control Procedures

1. Introduction
Technical access controls are built into information systems by IT system suppliers. To ensure confidential information is protected, this functionality must be supported by operational and managerial controls put in place by Volunteer Cornwall.

2. Purpose
The Access Control Procedures set out how Volunteer Cornwall will allocate, manage, and remove access rights to computer systems holding information so that only authorised personnel have access to use and share information held within those systems; and they aim to ensure that access rights are used appropriately by Volunteer Cornwall staff.

3. Scope
These procedures relate to access controls for computer-based information systems managed by Volunteer Cornwall to store client identifiable data. They therefore cover the allocation, management and removal of user accounts and the guidelines provided to Volunteer Cornwall staff to ensure they use the system appropriately.

4. Summary of technical access controls
Volunteer Cornwall uses domain login authentication with Kerberos V5 validation to secure login accounts. General user accounts are grouped as “domain\users” which gives access to their own saved documents, company shared files and access to networked facilities such as printers and the internet. The company shared folders and files can, if needs be, protected further by removing the “domain\users” access and only granting individual accounts access, this protects any sensitive information stored from being accessed by unauthorised users.

Domain access (e.g., login and logouts) is recorded in the server “Event Logs” along with any password changes and other account-based activity. Each event record is logged with the time and date of each occurrence.

5. Responsibility for user access management
Volunteer Cornwall has assigned responsibility for managing user access rights to the system to the IT Officer, who has administrator rights allowing access to management controls and areas. The unnecessary allocation and use of administrator rights is often found to be a major contributing factor to the vulnerability of systems that have been breached, therefore allocation of administrator rights to other staff can only be authorised by the Accounts and Administration Manager.

6. General
Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. During their induction to the system each user is given a copy of the guidelines on the appropriate use of computer systems (see Information Governance/14. Controls of Computer and IT Systems/321. Guidelines on the appropriate use of computer systems) and their user login details and is required to sign to indicate that they understand the conditions of access. A record is kept of all users given access to the system.

7. New permanent staff

When a new employee or volunteer joins the IT Officer arranges access to the system.

8. Temporary Staff or Volunteers

Temporary access is granted on a need to use basis. Such logons are granted by the IT Officer and are recorded and reported in the usual way. Temporary logons are identified by a specific login (e.g., TEMP01/GUEST02) and are time limited and deleted or suspended immediately when no longer required.

9. Change of user requirements

Changes to requirements will normally relate to an alteration to the level of access used or suspension of an account, e.g., if the user is on long-term leave, a volunteer who returns from time to time. Requests are made to the IT Officer and a record is kept of all changes.

10. Password management

Password management systems enforces a 90-day renewal, a 6 or more-character password length, a 5-password reuse policy and complexity methods using three out of the four following categories:

- Uppercase characters (A through Z)
- Lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, £, #, %)

Users may change their password at their own request.

11. Forgotten password

Where a user has forgotten their password, a replacement should be requested from the IT Officer, who issues a temporary, single use password which requires the user to reset their password on login.

12. Removal of users

As soon as an individual leaves Volunteer Cornwall, all his/her system logons are revoked either by locking the account or by changing the password. As part of the employee termination process senior managers inform the IT Officer of all leavers and their date of leaving. This also applies to volunteers.

13. Review of access rights

The IT Officer reviews all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons, which are identified, are disabled immediately and deleted unless positively reconfirmed.

14. Monitoring compliance with access rights

The management of access rights is subject to regular compliance checks to ensure that this procedure is being followed and that staff and volunteers are complying with their duty to use their access rights in an appropriate manner. Areas considered in the compliance check include whether:

- Only staff regularly working are registered as active users on the system.
- Allocation of administrator rights is restricted.
- Access rights are regularly reviewed.
- There is any evidence of staff or volunteers sharing their access rights.
- Staff are appropriately logging out of the system.

15. Approval

These procedures have been approved by the undersigned, and they will be reviewed on at least an annual basis and will consider any changes made to the technical access controls in systems.

Access Management Procedure

It is the responsibility of senior managers, alongside the IT Officer, to ensure each domain user account and email account in their department is current and accurate and not accessible to other users during and after their time at Volunteer Cornwall.

Request for change of account

When a change to an account is required, a request from a senior manager or Human Resources will be sent to the IT Officer via email stating the nature of the change. This can be adding a new account, deleting an existing account, or making a change to an account.

Creating account

On request of a new account for an employee or volunteer, the IT Officer will enter the new account details onto the domain server and allocate appropriate permission. This will allow the account access to its own user area and the file share space. An email account is also created at this point if needed for the user.

Changing/Locking accounts

The IT Officer will make any changes to an account on request by email from senior managers. This can involve changing the password, user details or even locking an account.
When the user of an account leaves Volunteer Cornwall, the IT Officer will either lockdown the account to prevent any further access or change the password to allow another user (e.g., Senior Manager) access to the account. Locking the account also disables access to the users email account.

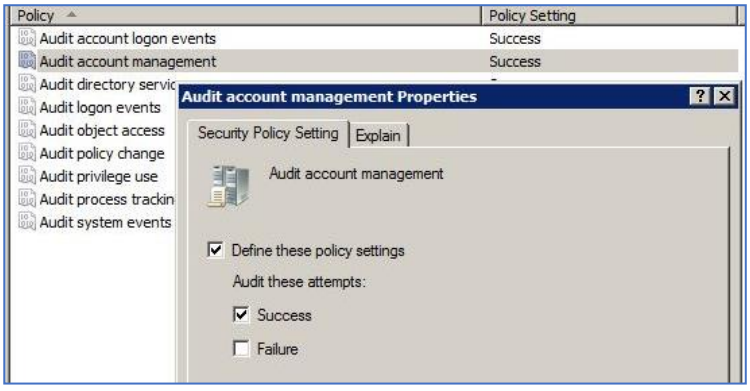
Deleting accounts

Once an account is deemed as no longer required, the senior manager involved will request to the IT Officer that the account be removed from the server. Once removed all account documents and settings will be deleted along with the email account and all its emails.

Event Logs / Record of change

The Volunteer Cornwall server policies are defined to record any changes to a user account. This security setting (see image 1) determines whether to audit each event of account management on the domain active directory. Examples of account management events include:

- A user account or group is created, changed, or deleted.
- A user account is renamed, disabled, or enabled.
- A password is set or changed.



1: Active Directory Policy Setting

When defined, this policy setting can specify whether to audit successes, audit failures, or not audit the event type at all.
Successful audits generate an audit entry when any account management event succeeds. When the IT Officer creates a new account, changes an existing account or deletes/locks an account, a record will be created in the servers event log (see image 2 below) to show details of the change.

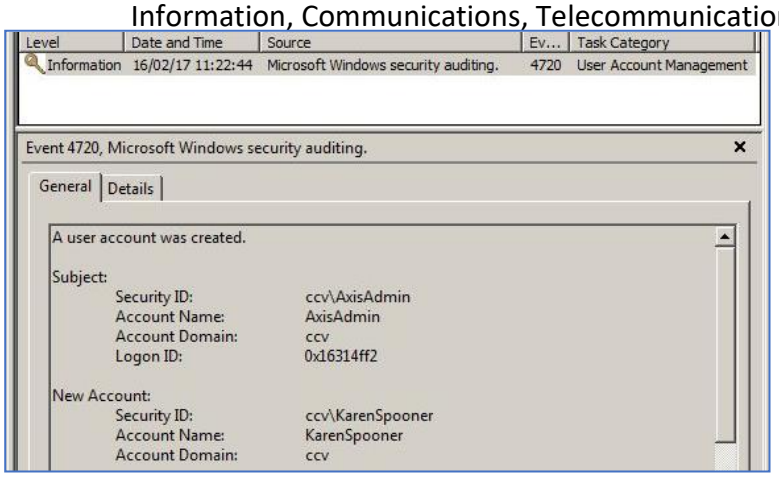


Image 2: Example of Event Log record

Control of Access to Internal IT Systems

Introduction

Control of access to Volunteer Cornwall servers and its internal IT systems are controlled using challenge/response authentication requests alongside the firewall/gateway security to protect the systems from unwanted traffic.

Internal/Domain access

Users connected internally to the local network within head office are required to sign in with a domain username and password to gain access to their domain user profiles. From there the user can connect to the Remote Desktop Protocol application, supplying their domain username and password to gain access to the user specific remote desktop session. Any user without accurate credentials will be denied access to any part of the internal IT systems. Due to user location, the remote desktop session connections within the internal network will bypass the Remote desktop gateway and connect directly through the local network.

All users requesting access this way must be a member of the "Users" domain group to be granted access, even with correct credentials. Only the IT Officer can grant these permissions.

External/Remote access

Users connecting to the internal IT systems while outside of the head office local area network (LAN) will be supplied with company equipment which will adhere to the ICT network security policy with company standard security/protection software for use with Volunteer Cornwall IT systems.

Remote Desktop users connecting externally will not gain access to their domain profile but will use the remote desktop connection (on their mobile device) to connect directly to their remote desktop session.

Connecting to a remote session externally requires Two Factor Authentication. 1) The Volunteer Cornwall server gateway will require its own set of credentials from the remote desktop application to allow access through the gateway to create a remote session, 2) which in turn requires domain login credentials which are subject to NTLM challenge/response protocol checks to allow access to the session.

Even if both "Two Factor Authentication" checks are passed and the user is <u>not</u> a member of the Volunteer Cornwall "Mobile Users" active domain group, access will <u>not</u> be granted.

ICT Networking Controls

This document identifies and describes the controls applied to all networks in accordance with the ICT network security policy.

Network Capacity Planning

The purpose of capacity planning is to ensure that server content can reach all users without delays or interruptions. A network that has been properly planned and configured can improve response time, data throughput and content availability.

Volunteer Cornwall uses a Fibre Broadband connection [300MB/s] to facilitate its Remote Desktop functionality and to give authenticated users access to internet and email. This gives significant bandwidth allowances to Volunteer Cornwall's low number of external remote desktop session users (no more than 10 at one time), allowing the highest functionality while remote working.

Network Security

Personal computers within Volunteer Cornwall Head Office domain site use an ESET NOD32 Antivirus Business solution to prevent malicious viruses, malware and other such files from being activated or downloaded from external sources. In addition, a Heimdal Security client is installed to scan internet traffic to protect users from Cyber-attacks. Mobile devices such as laptops employ a more robust Internet Security software solution (such as Norton Internet Security subscriptions) which as well as Antivirus software includes firewall solutions and invasion detection features to prevent unauthorised access.

The company domain server uses a Dreytek Vigor 2960 router/Firewall solution to provide protection from unauthorised connections and attacks. The firewall by default blocks all traffic on all ports, then has been configured to allow only essential traffic through by opening the required ports for specific data (e.g Port 3389 for Remote Desktop data, Port 433 for HTTPS).

Remote Desktop users require specific gateway server details and fully qualified domain name (FQDN) credentials to "dial in" and gain access to their remote sessions while outside of the Head Office network. These credentials are subject to NTLM challenge/response protocol checks to protect access. The user must also be a member of the domain servers "Remote Access" group policy, else authentication will fail.

File Storage / Group access

Within the domain environment each user is granted access to their own documents and the company file share space (allocated data drive/area where files can be stored for all users who have logged into the domain). Access to other user files is denied. Within the company file share space, specific folders can be locked down to prevent general access, these folders and files have their global "users" group removed and specific users are granted individual permissions to ensure only the specific users have access to protected areas on the file share space.

Use of Public Wi-Fi

Public Wi-Fi is available just about everywhere, from the local coffee shop to the hotels and airports you visit while traveling. Wi-Fi has made our lives a little easier, but it also poses security risks to the personal information available on our laptops and smartphones. Here is a helpful list of dos and don'ts you should follow if you plan to use public Wi-Fi.

Two Types of Public Wi-Fi

There are basically two kinds of public Wi-Fi networks: secured and unsecured. An unsecured network can be connected to within range and without any type of security feature like a password or login. Conversely, a secured network requires a user to agree to legal terms, register an account, or type in a password before connecting to the network. It may also require a fee or store purchase to gain access to the password or network.

Regardless of the connection type, you should always use public Wi-Fi with caution by taking some of these easy steps:

Please remember that these issues relate to and include the logging onto your emails and files through Office 365. This can also be accessed without your consent through public Wi-Fi.

Do connect to secure public networks whenever possible. If you're unable to connect to a secured network, using an unsecured network would be permissible if the connection requires some sort of login or registration.

Don't access personal bank accounts, or sensitive personal or client data, on unsecured public networks. Even secured networks can be risky. Use your best judgment if you must access these accounts on public Wi-Fi.

Don't leave your laptop, tablet, or smartphone unattended in a public place. Even if you're working on a secure Wi-Fi network, that won't stop someone from taking your property or sneaking a peek at your device.

Don't shop online when using public Wi-Fi. Shopping doesn't seem like it involves sensitive data, but making purchases online requires personal information that could include bank account and retailer login credentials. Shopping isn't something you want to do on an unsecured Wi-Fi network.

Do turn off automatic connectivity. Most smartphones, laptops, and tablets have automatic connectivity settings, which allow you to seamlessly connect from one hotspot to the next. This is a convenient feature, but it can also connect your devices to networks you ordinarily would not use. Keep these settings turned off, especially when you're traveling to unfamiliar places.

Do monitor your Bluetooth connectivity. Bluetooth in the home is an amazing feature on many smart devices. However, leaving Bluetooth on while in public places can pose a huge risk to your cybersecurity. Bluetooth connectivity allows various devices to communicate with each other, and a hacker can look for open Bluetooth signals to gain access to your devices. Keep this function on your phone and other devices locked down when you leave your home, office, or similar secured area.

If you have any concerns about accessing through public Wi-Fi, please use the philosophy, if in doubt, don't connect and access data.

Bring Your Own Devices (BYOD)

Introduction
Technology and business practices have moved on over recent years to a point, where people can and do use their own devices to access Volunteer Cornwall's IT systems.

By its very nature, BYOD is considered a data security risk and should only be used in certain circumstances, and if used, compliance with the terms of this document is required as a minimum, as we need to try and reduce risks as much as is possible.

Scope
For the purposes of this policy, the term "BYOD" includes, but is not limited to, smart phones, tablets, laptops, PCs, portable storage and any other fixed or mobile computing device.

The policy applies to all Volunteer Cornwall employees, visitors, volunteers, contractors, agents, and anyone who is using the Volunteer Cornwall IT services. The term "Officer/s" refers to anyone is this group of people.

Principles
Where a corporate device has malfunctioned and is not available, a user must ask IT for a spare machine before attempting to use personal equipment.

On no account, without prior written consent should a personal device be used on the Volunteer Cornwall IT system. If consent is granted by Senior Manager, it will be based purely on the business case for usage and will be logged on a database of the devices which are eligible to access the Volunteer Cornwall IT system. This database will be held by the Data Protection Lead.

In the event a personal device is given consent to access the Volunteer Cornwall IT System, the officer and owner of the device agrees to ensure that the operating system, any anti-malware, and security software on the device is the latest version and fully up to date.

Confirmation of this will be provided by IT after inspection of the device.

Officers must report any loss of a personally owned device to the Data Protection Lead, if it is used to access the Company's system, so that the risk of a data breach can be assessed.

Officer-owned devices that are also used for personal purpose should not be used to download personal or commercially sensitive data from the organisation.

System Availability
Officers can access Office 365 through BYOD devices, which allows access to emails, and One Drive, but no access to the corporate drives through the network, including the G drive and remote desktop. In addition, access to Teams, can also be gained with the downloading of an app through the Office 365 forum.

Volunteer Cornwall would request that no officers' accesses Teams through the app, as we are unable to secure the link. For access to Office 365 no officer should leave the system automatically logged on. Whilst this means that you need to remember log in details, in the event your device is lost or stolen, our data is protected, as access cannot be gained as easily.

When accessing your emails, or OneDrive, the company requests that no document is downloaded and stored on your BYOD device. Your BYOD should be configured to not allow the download and storage of documents.

Accessing non secure WiFi networks are covered through the Volunteer Cornwall Information, Communications, Telecommunications and Technology Policy, Annex J. Access through public WiFi. Please ensure you adhere to this policy around security and risks.

When leaving the employment or the end of a project, access to Office 365 will be terminated by IT, and the user will have no access to our systems. Prior to your leave date, if you have consent to use a BYOD, IT will request to check your personal device for any company related downloaded data. If any is found, this will be deleted.

Responsibility
Data protection and security is the responsibility of all staff, volunteers, and workers within Volunteer Cornwall, and all staff should consider the implications of their use of device.

All users of Volunteer Cornwall's IT must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects confidentially, integrity and availability, regardless of whether the devices used are Volunteer Cornwall or personally owned.

All officers are responsible for accessing and engaging with all mandatory Data Protection Training and any guidance issued.

Volunteer Cornwall takes no responsibility for maintaining, repairing, insuring or otherwise funding BYODs.

Volunteer Cornwall will not be responsible for any loss or damage resulting from any support given or advice provided.

It is the responsibility of any officer to obtain consent from a member of the Senior Management Team, prior to using their own devices on Volunteer Cornwall's IT Systems.