PO111 USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) AND SOCIAL MEDIA POLICY AND PROCEDURE

Policy

USE OF COMPUTER SOFTWARE AND HARDWARE
You are provided with access to a computer for the better execution and performance of your duties. The system is provided in the main for the sole purposes of communicating to our clients, volunteers and business contacts.

Time spent on the system is very valuable to us, as such we do not encourage you to use the system for personal e-mails or use of the internet being carried out during normal working hours. We are however, happy for you to use the system during your normal lunch break and before or after working hours have ceased. However, extreme caution must be exercised in regard to viruses and data from sources which you have not been authorised to process.

You are provided with your own login details and password in order to access our computer systems. In addition, depending on the nature of your position, you may be provided with an iPad, laptop or other device for the better execution of your duties.

Guidance

It is vitally important you are aware of your responsibility in regard to using our system; that is we will not permit you to use your computer, laptop or other device for the purposes of:

- Online gambling and/or game playing
- Accessing pornographic or other undesirable Internet sites, as determined by CVS Falkirk.
- Posting confidential information about other employees, the organisation, or its clients, unless you are required to do this as a function of your job and it is detailed in your job description
- Copying information, which is considered private, personal or intellectual capital of CVS Falkirk.
- Downloading any information onto a CD Rom, floppy disc, USB pen or other media devices unless it is for the better performance of your duties as it is accepted that some individuals will need to download specific information albeit within the parameters of their specific tasks and duties
- Undertake any blogging activities, unless you are required to do this as a function of your job and it is detailed in your job description
- Access to any social media, unless you are required to do this as a function of your job and it is detailed in your job description
- If you require access to a social media site for genuine work reasons, this must first be agreed in writing by your Line Manager or the CEO.
-

Every computer holds extremely valuable data, which must always be treated as highly confidential. As such you must be aware of the following:

- Some software in use is under licence from the producers and may not be copied from one computer to another
- No software may be copied, installed, removed, altered or used on our computers without prior written authorisation from the CEO
- Any downloaded materials may be sporadically accessed. However, where we suspect misuse, you will be notified and access duly taken prior to your consent. Thus we reserve the right to investigate such activities without breaching the Data Protection Act 1998 or The Regulations of Investigatory Power Act 2000. The data may then be used as evidence for either disciplinary or criminal investigations.
- Any data, documents, forms publications images or presentations developed by you during your employment with us remains the sole property of CVS Falkirk and may not be copied or removed without prior written consent from us
- Our systems are protected from unauthorised access by the use of passwords
- Passwords must never be given out to any person who is not an employee or volunteer with us, or who is not permitted to have access to our system.

You are required to log on to the computer system using your own password, which must remain confidential at all times unless prior written authorisation from us has been obtained. Anyone found disclosing his or her password by any communication method or who uses another person's password to log on to the computer system, with or without that person's permission will be liable to summary dismissal for gross misconduct.

When leaving a computer unattended in an area occupied, or likely to be occupied, by other persons, (for whatever reason) you must either:

- lock your device
- log off your device
- shut down your device

to prevent other people utilising the organisation's computer systems under your login. Leaving a device accessible to other people could lead to disciplinary action.

VIRUSES AND OTHER MALICIOUS SOFTWARE

Viruses etc. pose a serious threat to the organisation's computer systems. The organisation has anti-virus software. It is a strict rule that no software or documents or files may be loaded onto any computer or similar device until it has been checked for viruses by our retained IT Services organization. Any report of a virus or suspected virus must be forwarded to the designated service desk for the organisation's computer support.

NO ATTEMPT SHOULD BE MADE TO BYPASS ANTI-VIRUS SOFTWARE CHECKS OR TO DISABLE OR ALTER ANY ASPECT OF THE ANTI-VIRUS SOFTWARE'S OPERATION AND/OR CONFIGURATION.

BACK UP
All central computer systems and filesare backed up on a regular basis. Laptops and PCs can fail to operate, as such vital information can be lost, therefore all data must be protected. All master copies of documents must remain on the network, and not stored on any other devices.

Company Laptops and other devices
A number of laptop computers and other devices are available for use when you are working at home or out of the office. However this is subject to:

- Authorisation having been sought and duly given by the CEO or your Line Manager
- The device never being left unattended or in a manner where security of the information could be and/or is put at risk
- When transporting the device in a vehicle it must be stored in a locked boot or glove compartment where possible or else hidden from view and locked
- Reasonable care being taken to avoid damage or loss
- Any accidental loss or damage being immediately reported to the CEO or your Line Manager
- Minimal data being held on laptops for reasons of client protection, confidentiality and Data Protection.

On leaving the organisation's employment, and at any other time at management request, you are required to hand in all our equipment, information and data held in computer-usable format.

MONITORING, SECURITY AND PERSONAL USE
Personal use of our Internet and E-mail systems is strictly prohibited during working hours, therefore it should be noted that we reserve the right to monitor and record your usage of the Internet and e-mail system and any files stored on your computer at any time without first seeking your consent.

MONITORING
We reserve the right to monitor and record the use of our systems to ensure:

- Compliance with all legislation pertaining to e-commerce and IT
- That you are not downloading pornographic data. (If found doing so, you will be subject to both our Disciplinary Procedure and criminal prosecution, under the Obscene Publications Act 1950).
- CVS Falkirk never mislead the general public or clients
- CVS Falkirk is never brought into disrepute
- Unsolicited e-mails are handled in the appropriate manner (The Government has left the matter to self-regulation)
- You must ensure you protect our ethicality and integrity at all times.

It is worthy of note that you may not be notified when you are being monitored.

No telephone calls, e-mails or Internet use will be intercepted at the immediate point of use, unless there is a risk or potential risk to you, other employees, a client or ourselves. Monitoring will however be enacted albeit within strictly controlled environs, using the appropriate technology for data logging.

Any electronic and downloaded materials may be sporadically accessed. However, where misuse is suspected, you will be notified and access duly taken prior to your consent. Thus, we reserve the right to investigate such activities without breaching the Data Protection Act 1998. The data may then be used as evidence for either disciplinary or criminal investigations.

In summary, although we are happy for you to use the system in your own time, we respectfully ask you to keep any communication in connection with personal business interest to a minimum or if possible avoid using our system in this regard. In some instances, abuses of the organisation's resources may constitute a criminal offence.

As such the organisation reserves the right to, and in many cases is legally obliged to, report suspected illegal activities relating to the use of our computer resources to the relevant authorities. Some legislation places a requirement on the organisation to monitor for, and report, any activities which are, or could be, illegal. As a result, the organisation or another party may instigate legal proceedings against anyone suspected of participating in, or having knowledge of, any such activities.

SOCIAL NETWORKING

The growth of computer use and internet expansion has led to an increase in the use of blogs and social networking sites. Whilst employees may choose to indulge in this practice at home the company has strict guidelines on the use of such sites:

- The use of social networking sites & blogs must not be allowed to interfere with or bring into disrepute the conduct of CVS Falkirk or its good name or reputation
- No blogs or social networking profiles whatsoever will be created or updated on ANY computer owned and operated for company business.
- No employee must directly or indirectly refer to or implicate the organisation, its staff, or any of its customers on any blog or social networking profile created by them.

Employees contravening this rule will be subject to the Disciplinary procedure PO51.

Use of our computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems.

USE OF EMAILS

CVS Falkirk has software and systems to monitor and record all e-mail usage and may, from time to time, inspect files stored in private areas of the network in order to assure compliance with this Policy.

The organisation's e-mail is not a personal e-mail facility and you are not generally permitted to use the organisation's e-mail address except for legitimate business purposes or for limited personal use where this is infrequent and the content does not constitute a misuse of the system (as defined below).

The use of the organisation's e-mail address for personal reasons must only be used when communication with, or about, subjects is not likely to bring harm or ill repute to the organisation, its directors, employees, volunteers or clients either directly or indirectly.

Any information which could be considered confidential or sensitive by the organisation must not be communicated out with the organisation.
Misuse of E-mail facilities may result in disciplinary action up to, and including, dismissal.

Examples of misuse include, but are not limited to, the following:

- Transmitting obscene, profane or offensive material
- Accessing or transmitting sexual materials
- Transmitting or displaying messages, jokes, or forms which constitute harassment or create an intimidating or hostile work environment
- Using company communications systems to set up personal businesses or send chain letters.

USE OF INTERNET ON COMPANY DEVICES

CVS Falkirk has software and systems to monitor and record all internet usage.

You are not permitted to use the organisation's internet facilities during working time for personal purposes, unless you have obtained prior authorisation from your Line Manager or the CEO.

The display of sexually explicit or otherwise offensive images, documents or text on any organisational system, even for personal use out with working hours, is a very serious breach of our rules, and could lead to summary dismissal.

If you find yourself accidentally connected to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately and report the incident to your Line Manager or the CEO.

Use of our internet facilities which results in the misuse of our assets or resources, sexual harassment, unauthorised public speaking or the misappropriation or theft of intellectual property is also strictly forbidden and could lead to summary dismissal.

USE OF PERSONAL DEVICES

You are not permitted to use your own personal device during working hours, except during your official breaks eg lunch time, and only then if you are away from your desk.
Personal devices of every type must not be on your desk or workplace, but should be shut away in a drawer during working hours.

You are not permitted to use personal devices in the office **at any time** to download large files, such as videos, music files, films, television etc or for live streaming such as Netflix etc. This will be considered a misuse of company assets and could lead to summary dismissal.

ACCESS TO COMPANY INFORMATION OUTWITH THE OFFICE

Our email and file sharing services are now 'in the cloud' which means they are accessible from anywhere and on any suitable device. This can be particularly useful if you are unable to get to the office for any reason, such as during bad weather, or if you need to access information for a presentation or a meeting.

It is imperative that security of data remains paramount, and the following rules must be observed at all times without exception:

- Never access the organisation's systems from a public terminal eg a pc in a public place such as an internet café
- After accessing the organisation's sytems, always delete your browing history
- Do not save any data to the local device; all work must be undertaken in the cloud environment only
- Do not print anything to printers accessible to the public
- If any device you have used to access the organisation's data is lost or stolen or compromised (available for someone else to use) you must inform the CEO immediately
- Do not permit any software on any device to retain your login id or your password under any circumstance
- Always log out and close down any application before shutting down the device.

Above all, be careful and vigilant about use of your login and password, and never leave your device logged in and unattended.

Related Policies:	PO51 Disciplinary	
Related Documents:	none	
Version:	2.0	
Published:	April 2015	
Review due date:	April 2017	Review Completed: June 2016
Review due date:	June 2018	Review Completed: