ICT policies

Supporting charities, volunteers and communities
wcva
Yn cefnogi elusennau, gwirfoddolwyr a chymunedau

Procurement policy

Hardware purchases – all hardware to be purchased must have a clear business benefit, once this is agreed an electronic hardware/software request form must be completed and submitted to WCVA ICT. Once this is received WCVA ICT will get a quote for the equipment in line with WCVA's purchasing policy and submit this to the requester for authorisation.

Software purchases - all software to be purchased must have a clear business benefit once this is agreed an electronic hardware/software request form must be filled in and submitted to WCVA ICT. Once this is received WCVA ICT will get a quote for the software in line with WCVA's purchasing policy and submit this to the requester for authorisation.

Infrastructure purchases – infrastructure purchases are agreed and purchased by WCVA ICT only; any networking device connecting to WCVA's network must be purchased through WCVA ICT. All purchases must be in line with WCVA's purchasing policy.

Websites – all WCVA websites must be provisioned and procured through WCVA ICT. All intranet websites must be hosted internally on WCVA's servers and all external websites must be hosted on WCVA's co-location box situated at BT's IDC in Cardiff Bay.

Application development – all WCVA application development must be provisioned and specified by WCVA ICT.

WCVA only uses the following operating system versions on its agreed WinTel hardware:

Desktop/Laptop – MS Windows 2000/XP
Network operating System – Windows server 2000/2003
Unix/Linux operating system – CentOS

WCVA printers – all WCVA printers must be HP and covered by a current HP support pack. Extended support packs are charged back to their prospective end users.

Security policy

Introduction

WCVA has a duty to protect its information assets and thus to ensure business continuity and minimise the adverse effects of security incidents. Information assets and the ICT systems that support them are becoming increasingly more vulnerable as the potential for wider accessibility is facilitated via more powerful computers and communications networks.

Information takes many forms and includes papers, databases, films, computerised images, view foils, tapes, diskettes, memory sticks, data keys *etc*. From a security perspective appropriate security protection should be applied to all types of information and information media.

WCVA's information strategy

WCVA's information strategy is to allow information to flow as freely as possible and that access to information should be permitted on the basis of "need to restrict" rather than "need to know". These policies do not conflict with the need to protect sensitive information and to safeguard the accuracy and completeness of information and computer software.

Information security

Information security management has three basic components:

Confidentiality: Protecting sensitive information from unauthorised disclosure or copying.
Integrity: Safeguarding the accuracy and completeness of information and computer software.
Availability: Ensuring that information and vital services are available to users when required.

Information security policy; Purpose, aims and principles

WCVA's Information security policy is intended to safeguard WCVA and WCVA's staff of intellectual property rights from information security related incidents and any consequential action, loss of income or damage.

The principles set out in the paragraphs which follow apply to WCVA's information and information systems.

Responsibility

It is the responsibility of all users of WCVA's information sources and systems to comply with statutory, WCVA and ICT policy instructions regarding the safeguarding of information and information media.

Access

All staff having privileged access to sensitive information are responsible for ensuring that access controls and the information obtained via such controls is not compromised by; revealing or failing to protect password information; revealing or allowing access to information by persons not authorised to have it and failing to take reasonable precautions against unauthorised access *e.g.* leaving a workstation unattended which is logged-in or failing to secure sensitive documents.

Virus prevention

The so-called computer viruses include "network worms, Trojan horse, logic bombs" *etc* are malicious techniques to make unauthorised modifications to computer software. Personal computers are particularly vulnerable to these types of attack. To minimise the risk of virus infection licensed and authorised software only may be used on WCVA systems. Further protection is provided by routine updates of virus detection software and e-mail gateway scanners.

System usage

All computer systems and network access provided for use by WCVA staff are subject to all WCVA ICT policies.

Privileged systems usage

Users having privileged access and/or systems update rights may not use such privilege for personal gain, or deception by the creation of bogus records; fraud via use of unauthorised software or for any purpose other than legitimate WCVA business.

Replication

All staff must comply with WCVA instructions and limitations on the copying of material subject to copyright.

Continuity planning

All WCVA information systems are subject to potential loss of data due to failure of software or hardware media. It is the responsibility of the ICT Unit, in the case of central systems and users for local systems, to ensure that regular back-up copies of essential data are made and stored in a safe location, remote from the system. Computer media *e.g.* disks, should not be left lying around in offices and staff using personal data at home must ensure that both PCs and media are secured after use.

Disaster recovery

There is a risk that an entire system may be lost as the result of a disaster *e.g.* fire or flood. For central systems where an alternative system platform and software may not be readily available, then other provision will be made on the basis of a risk assessment analysis by the lead department *i.e.* Finance for the finance system.

Conduct and use of computer systems and network at WCVA

WCVA provides computer workstations and communications network access to a variety of services which are hosted either by WCVA or by external agencies via wide area network facilities *e.g* Internet. The conditions of use are:

Computer systems and networking facilities shall be used only for work and activity approved by WCVA.

Access

No attempt shall be made to access WCVA systems, networks or databases unless legitimate authorisation has been granted.

No attempt shall be made to access the systems and networks of other establishments either, within the United Kingdom or elsewhere unless the service required is a public or open access facility, and authorisation has been obtained from the system/network service provider.

Usage

Systems and networks are not to be used for commercial purposes, nor to obtain external funding unless written permission had been obtained from the relevant Cluster Coordinator.

Computer systems and networks shall not be used to engage in any activity liable to cause offence or to obstruct other users of WCVA systems or users elsewhere. This includes the deliberate introduction of *viruses* into WCVA systems and networks.

Computer systems and networks may not be used to access, display, print or distribute slanderous, libelous or knowingly untruthful information or material of an illegal nature.

Copyrights and intellectual property rights must be respected by all WCVA computer system users and only third party software which has a current licence, or is in the public domain can be authorised for use. The unauthorised copying of software in breach of licensing agreements may result in disciplinary action.

Security

A password is the personal property and responsibility of the individual to whom it is issued. When issued with a password allowing access to information on systems and networks, a user may not divulge such password information to any other person whomsoever.

Computer systems and networks may not be used to access, download or store personal information which is subject to the Data Protection Act without prior authorisation from the relevant Cluster Coordinator.

Backup / restore policy

WCVA's backup strategy covers all central data and is backed up fully every weeknight as follows:

All S:\ and U:\ drives are included in a full backup on weeknights with a 24hr previous copy held offsite for contingency purposes.

All e-mail / Public folders are included in a full backup on weeknights with a 24hr previous copy held offsite for contingency purposes.

All WCVA databases are included in a full backup on weeknights with a 24hr previous copy held offsite for contingency purposes. Including:

- IDRIS
- Sage 200
- GALS
- Sage Payroll X 2
- Mytas
- Visual Personnel
- Target BlueChip

WCVA Data that is saved on desktop machines must be copied and/or backed up to WCVA's central services to ensure it can be recovered. WCVA information held on your desktop or in 'My Documents' only is not an allowed data storage configuration. You must use the server configuration to share WCVA information with other users (S:\) or store personal/private information in you user (U:\) drive.

WCVA Data that is saved on laptops/PDA's/Blackberry's or any other portable storage device must be periodically backed up to WCVA's central services to ensure it can be recovered (see laptop/PDA/Blackberry policies).

IT pool equipment loan

The following ICT pool equipment is available for loan:

Laptops X5 (4 Cardiff 1, Colwyn Bay)
VGA projectors X5 (2 Cardiff, 3 Colwyn bay)
Video conferencing equipment X 2 (1 Cardiff, 1, Colwyn)
Teleconferecing equipment X 2 (1 Cardiff, 1, Colwyn)
Digital camera X 1 (1 Cardiff)

IT pool equipment can be booked out providing it is available from WCVA ICT. Availability can be checked in the office resources public folder in Outlook.

It is the responsibility of the end user to set up the equipment for use. Procedures for using the equipment can be found at S:\ICT Unit\Procedures\data projector.doc. If training is required this will be provided either via previously trained colleagues or where not possible WCVA ICT.

Checking the equipment before use is the responsibility of the end user who wishes to borrow it.

If you discover any of the equipment is faulty this must be reported to WCVA ICT immediately.

WCVA's insurance policy only covers equipment in cars if it is stored out of site and locked in the boot. Any equipment that is stolen from elsewhere in a car is the responsibility of the person who left the equipment there. This also applies to equipment left unattended and unsecured.

If any equipment is lost or stolen it must be reported to WCVA ICT immediately.

ICT monitoring policy

WCVA resources including all related equipment, networks, and network devices are provided for authorized WCVA use. WCVA computer systems may be monitored for all lawful purposes, including ensuring authorised use, for management of the system, to facilitate protection against unauthorised access, and to verify security and operational procedures.

All information placed on or sent to this system may be subject to such monitoring procedures. Use of WCVA's system, authorised or unauthorised, constitutes consent to this policy. Evidence of unauthorised use collected during monitoring may be used in a court of law.

The following information may be audited and monitored for WCVA purposes:

Telephones internal/external calls etc.
Mobile Phones (including location monitoring*)
E-Mail (transactions and content)
Internet access
Database transactions
User account transactions

Data access audits
Flexi sheets
CCTV cameras
VPN access
Outlook Web Access

* Location monitoring is a new facility to track the whereabouts of mobile phones by triangulating the base transmitter signals. Services include telling you how to get to the nearest cash machine or chemist; allowing a staff member to identify the location of his or her colleagues; and assisting WCVA with the security of lone workers.

External development / 3rd party data access policy

All Data extractions databases leaving WCVA systems for third parties must be authorised by either ICT manager or database administrator.

The form for this can be found on S:\ICT Unit\Policies.

Instant messaging policy

WCVA does not allow any form of instant messaging software to be used on any of its systems. Installation or configuration of any IM software is a serious breach of the ICT Policy.

New ICT user policy

A *New user request form* must be filled in as soon as the starting date of the employee is known. WCVA HR informs new line manager of responsibility.

An electronic form is available through Outlook public folders for this purpose.

Staff leaving / dismissal policy

A *Staff leaving form* must be filled in as soon as the finishing date of an employee is known. In the advent of a disciplinary/dismissal a form must be completed immediately.

Accounts are disabled at the end of the final day of the employee. All standard accounts and any related information is kept for 1 month. Any further archival must be stated on the staff leaving form. See ‘Data Archival’ for further information.

WCVA HR informs line manager of responsibility. A form is available on the shared drive S:\ICT Unit\

Data archival policy

All archived material is kept for the requested period in a secure fireproof safe and a copy is sent to the person requesting the data to be archived for their use.

Roaming user/laptop/palmtop/tablet PC policy

Only WCVA registered laptops/palmtops/tablet PC’s may be used on WCVA’s network. These devices must be brought into WCVA offices and plugged into the network at least once every month to ensure that all security patches and virus definitions are uploaded to the laptop.

All data on the laptop must be copied to the correct S:\ U:\ drives during the monthly visit. Information that is deemed to be confidential is the responsibility of the laptop user. It is recommended that any important files are backed up to WCVA shared resources S:\ and U:\ drives immediately. WCVA ICT cannot be held responsible for data lost from these devices.

If information held on a laptop is legally binding such as financial information this is to be copied to WCVA’s central network immediately through VPN access.

WCVA’s insurance policy only covers laptops in cars if the laptop is out of site and locked in the boot. Any laptop that is stolen from elsewhere in a car is the responsibility of who left the laptop there. This also applies to equipment that is left unattended and unsecured.

If a laptop is lost or stolen it must be reported to WCVA ICT immediately.

Blackberry’s/PDA’s/Smartphones/Pocket PC’s

Only WCVA registered Blackberry’s, PDA’s, Smartphones, and Pocket PC’s may be used on WCVA’s network.

All data on the any of the above devices must be copied to the correct S:\ U:\ drives at least monthly. Information that is deemed to be confidential is the responsibility of the user. It is recommended that any important files are backed up to WCVA shared resources S:\ and U:\ drives immediately. WCVA ICT cannot be held responsible for data lost from these devices.

If information held on any of these devices that is legally binding such as financial information this is to be duplicated to WCVA’s central network through the chosen synchronization method.

WCVA’s insurance policy only covers these devices in cars if they are out of site and locked in the boot. If they are stolen from elsewhere in a car it is the responsibility of end user in question. This also applies to equipment that is left unattended and unsecured.

If any of the above equipment is lost or stolen it must be reported to WCVA ICT immediately.

Data-Key/Pen and removable media policy

Only WCVA registered data keys/pens may be used on WCVA’s ICT network and only for WCVA agreed content transferal purposes. Information that is deemed to be confidential is the responsibility of the data key user. Data keys/pens memory is volatile and it is recommended that any important files are backed up to WCVA shared resources S:\ and U:\ drives. WCVA ICT cannot be held responsible for data lost from these devices.

If a data key/pen is lost it must be reported to WCVA ICT immediately.

iPod/MP3 player policy

Any MP3/WMA/iTune/mobile phone music player, such as an iPod, Sony Walkman, or Creative Zen *etc* are not allowed to be connected to WCVA's desktops/servers/laptops/network without prior permission from WCVA ICT.

It is also a copyright issue to have any MP3/WMA/iTune files on your desktop PC or WCVA shared resources if you do not have the original media the artist(s) intended for purchase or the track in question has been downloaded from a reputed website which uses industry agreed DRM measures.

A weekly script is used to identify and delete unwanted music files on both S:\ and U:\ drives. Files discovered will be removed without notice.

Colour printer policy

WCVA's colour printer must only be used for documentation that it is either essential or adds some business value through colour in its output.

Internet acceptable use policy

Permitted and prohibited Internet services

E-mail

Permitted uses

- Sending and receiving email messages with enclosures (file size less than 10MB) for business purposes. Emails with attachments over 300K going to large groups must be sent after 4pm.
- Sending and receiving short text messages with no enclosures for non-business purposes.

Prohibited uses

- Forwarding email chain letters.
- Sending or arranging to receive mail enclosures greater than 10MB.
- Sending or arranging to receive mail enclosures for personal reasons.
- Having a continuous dialogue with other e-mail users both internally and externally.
- Sending sensitive information by email over the Internet.
- Forwarding virus/security/phishing alerts to anyone other than the ICT unit.

Mailbox size allowances

Standard mailbox sizes are as follows

- Mailbox gives warning 150MB
- Mailbox prohibits sending 170MB
- Mailbox prohibits receiving 180MB

Mailbox manager

Mailbox manager runs weekly and removes the following:

- Inbox (and subfolders) – not cleaned
- Sent items – 30 days old removed
- Calendar - 30 days old removed
- Journal - 5 days old removed
- Deleted items - 30 days old removed
- System cleanup – 5 days old removed

Mailbox retention

- All mail is kept recoverable for 30 days after it is removed from the deleted items folder unless it is manually permanently deleted.
- All mailboxes are kept for 20 days after they are deleted.

Out of office replies/e-mail rules forwarding to the Internet

WCVA e-mail system is configured to allow ‘out of office’ replies to Internet mail recipients.

- Staff must ensure that when they are out of the office that either there ‘out of office’ reply is switched on (see ‘out of office’ best practice below) with the relevant alternative contact information included or alternatively use a mail forwarding rule to forward the request on to an internal colleague.

WCVA’s e-mail system does not allow any forwarding rules to the Internet for the following reason:

- Using mail forwarding to the Internet increases the possibility of causing a mail loop which could bring down WCVA’s mail servers.

Out of office best practice

- For privacy and security purposes WCVA staff shouldn’t say how long they are out for nor why they are out. They shouldn’t include their signature file as this gives away too much information and they should include the name of an alternate contact along with the telephone number.

The following is an example of a reasonably safe and yet informative Out of Office Reply:

“Thank you for contacting me - unfortunately I am away from my email right now but I will reply to you on my return. In the meantime, if you need some assistance, please call John Doe at 555 1234.”

Unsolicited commercial e-mail (Spam) filtering

WCVA e-mail system is integrated with a 3rd party spam filtering/virus detection solution.

- All incoming mail is scanned for viruses, banned attachment types, and scored regarding possibility of spam content.
- Viruses are stripped and placed in a quarantine area accessible by WCVA ICT only.
- Banned attachment (non WCVA business use) types are placed in a quarantine area accessible by WCVA ICT only. These include executables, batch files, music files, video files, multimedia files etc. *See prohibited e-mail usage regarding personal e-mail enclosures.
- All users have access to their own personal message centre to manage quarantined e-mail.
- All users receive a quarantined spam digest at 07:00 each morning. Mail that is stripped as a false positive can be delivered from here or dismissed as spam from your message centre.
- Once a false positive is delivered from the message centre you are prompted if you wish to whitelist it on your personal filter for future purposes. If it is delivered from the e-mail digest you will have to manually whitelist via the message centre.
- All spam unmanaged via the message centre or e-mail digest will be automatically deleted after 2 weeks.
- Any spam scored as blatant spam is dropped and will not show in your quarantine area.
- All users have the facility to manage their own allowed and blocked sender lists.

Web

Permitted uses

- Any user approved for Web access may connect to and view any Web page for well-defined business purposes within the flexi scheme.
- Any user may print Web pages.

Prohibited uses

- Installation of Web server software on any PC attached to the corporate network without written permission from ICT unit.
- Connection to Web sites related to sex, illegal drugs, criminal skills, hate speech, online gambling,
- Connection to sports, entertainment, online merchandising, humour, or job search. In business hours (recorded in WCVA's flexi scheme).
- Connection to any site for non-business reasons during business hours (recorded in WCVA's flexi scheme).

FTP downloads

Permitted uses

- Any user approved to download files from a particular site may download files from that site, IT has approved any software installed on user's workstation, and purchase of any required software license is approved.

Prohibited uses

- Downloading any file from a non-approved FTP-site; permission to download files is granted on a site-by-site basis, and permission will be granted only for trusted, major commercial sites.
- Downloading software without approval to purchase required license.
- Downloading from any site for non-business purposes at any time.

USENET Newsgroups

Permitted uses

- Any user with approved access to Usenet newsgroups may access newsgroups that have been previously requested and approved, if such access is for business purposes.

Prohibited uses

- Accessing any newsgroup for non-business reasons.
- Submitting messages to newsgroups.
- Accessing newsgroups related to sex, illegal drugs, criminal skills, hate speech, online gambling.

WCVA staff are encouraged to use their work e-mail address for personal e-mail outside core office hours that are not reflected in their flexi-sheets. Please note that all Internet activity logs will be passed to the relevant line managers.

Access to personal e-mail accounts (for example Hotmail.com, Tesco.net, Breathe.com) using WCVA's computer system is not permitted without specific authority to do so (which will be granted only by line managers for a specific purpose i.e. If WCVA's own computer system is down). Using personal e-mail accounts causes a security breach as WCVA receives e-mail that is not passed through WCVA's virus scanners/mail gateway.

All WCVA staff are encouraged to use WCVA's Internet facilities outside office hours (this includes lunchtime) for any Internet service/site that is not considered to contain dubious content/services. All sites with dubious content (*i.e* pornography, gambling, terrorist *etc*) should not be visited at any time; any occurrences in the activity logs in these areas will be passed to the relevant line managers.

Internet filter policy

WCVA’s Internet filter has categorisations of sites and allows the following access times –

Totally banned site categories

Anonymisers, cults & occult, extreme and violence, hate speech, malicious code, spyware, streaming media, criminal skills, personal e-mail, hacking, weapons, XXX related sites (Pornography)

Working day banned site categories (all hours except between 12:00 - 14:00)

Chat, entertainment, humour, job search, military, gambling, personal/dating, shopping, travel

Lunch (12:00-14:00)

All site categories minus total ban list.

Reporting mis-categorised sites

Mis-categorised sites may be reported to WCVA ICT who will check the validity of the request and then re-categorise if necessary. Sites can be reported by copying and pasting the address line (URL) from the WCVA banned page. This provides us with the full address of the site banned and also the category that it was banned from.

Category exemption policy

Exemption from certain site categories such as 'travel' can be authorised by an end users line manager in writing. With any exemptions it is the responsibility of the line manager to ensure that the exempt category is only used for work purposes by utilising the information in the monthly Internet access reports.

RSS Newsfeed / Newsgroup policy

WCVA allow the use of both RSS feeds and Newsgroups the former being the preferred method of accessing news services. WCVA only uses the outlook plug-in 'IntraVnews' and Microsoft IE7 newsreader as its RSS news feed reader. Newsgroups where authorised can be configured to work in Outlooks public folders.

Peer to peer (P2P) software policy

WCVA does not allow any form of peer to peer networking software on any of its systems such as: Kazaa, Bit Torrent, Morpheus, and iMesh *etc*.. Installation or configuration of any P2P software is a serious breach of WCVA's ICT Policy.

Data Protection

The Data Protection Act 1998 imposes statutory conditions for the maintenance of personal data on WCVA computer systems including data held by individual members of staff on PCs. It is an offence to use or disclose such data other than within the provisions of Act. Staff may use or store work related data on individual PC's at home for WCVA purposes only.

It is the responsibility of the staff to ensure that any personal data held is consistent with the WCVA Data Protection Policy and other relevant WCVA polices, and the eight data protection principles. If in doubt contact the ICT Manager or Data Protection Compliance Officer.

Data protection principles

The following are the eight data protection principles, which WCVA seeks to uphold:

1. Obtain and process personal data fairly and lawfully.
2. Hold personal data only for the purpose, listed in WCVA's notification.
3. Use the personal data only for the purpose and disclose only to the people, listed in WCVA's 'notified' entry.
4. Only hold personal data which are adequate, relevant and not excessive in relation to the purpose for which the data are held.
5. Ensure personal data are accurate and, where necessary, keep up to date.
6. Hold personal data for no longer than is necessary.
7. Allow individuals access to information held about them and, where appropriate, correct it or erase it.
8. Take security measures to prevent unauthorised or accidental access to, alteration, disclosure, loss or destruction of personal data.

The current WCVA Data Protection Policy is available from the WCVA website and the Data Protection Compliance Officer. Administrators and unit leaders have particular responsibility to ensure that each unit is compliant with data protection legislation and the Policy; this includes the induction of new staff.

Defunct / end of use equipment recycling policy

WCVA ICT endeavours to, where possible, pass on defunct PC's to Business in the Community for use within the voluntary sector and recycle any equipment that cannot be passed on.

All PC Hard drives must be wiped by WCVA ICT before re-use or recycling.

ICT support policy

WCVA ICT endeavours to provide a friendly professional ICT support service for all WCVA staff members.

If you discover you have a fault the preferred method of reporting the fault is through the outlook electronic forms that have been created for this purpose. If the fault prevents you from using these forms you can either get someone else to report the fault or use the paper fault report forms at S:\ICT Unit\Forms.
When filling in a form it is important that you prioritise the fault correctly. WCVA ICT will aim to resolve all issues as prioritised below.

All non-urgent events will be prioritised with WCVA's ICT work packages.
All urgent desktop support events will be responded to within eight hours.
All system down desktop support events will be responded to within four hours.

VPN / remote access policy

All users of remote access systems must ensure that the station they are using to access WCVA's systems is secure and that they do not leave the station unattended and logged in.

All staff having privileged access to sensitive information are responsible for ensuring that access controls and the information obtained via such controls is not compromised by; revealing or failing to protect password information; revealing or allowing access to information by persons not authorised to have it and failing to take reasonable precautions against unauthorised access *e.g.* leaving a workstation unattended which is logged-in or failing to secure sensitive documents.

ICT reporting policy

ICT project reports are delivered through the WCVA quarterly reporting structure associated with WCVA 5 year business plan.

ICT detailed project reports are delivered to the WCVA audit committee quarterly.

ICT operational monthly reports are delivered to WCVA cluster coordinators within the first week of the month. The reports include:

Telephone statistics
Internal e-mail statistics
External e-mail statistics
Website visitor statistics www.wcva.org.uk www.volunteering-wales.net
Website download statistics www.wcva.org.uk
Spam filter statistics

Internet access reports are automatically e-mailed to line managers on the first of each month. See Internet filter policy for details.

Declaration

I have read and fully understand that failure to comply with WCVA's ICT policies (15/02/2007) may result in suspension or withdrawal of access to WCVA computer systems and network facilities and may also render me liable to disciplinary proceedings.

Signed ______________________________ **Date** ____________________

Print name ______________________________