Caring Hands in the Vale

Information Communication Technology (ICT) Policy

Computer Usage: Code of Practice

Caring Hands in the Vale encourages the use of ICT, including e-mail and the internet, for legitimate business purposes. It is a condition of employment that employees and volunteers comply with all requirements of this section relating to:

Information security

The use of the organisation's computer systems

The internet, email or telephone

Misuse of the organisation's technology and communication facilities may subject you to disciplinary action which, in serious cases, can result in your summary dismissal.

Software

Only software which has been provided and installed from a company approved source may be used. There are copyright implications in using other software, which exposes both yourself and Caring Hands in the Vale to prosecution.

All software must be checked and installed by the designated ICT Officer. Any installation of software by any other employee or volunteer subjects the ICT network to instability. This may mean a possible breach of confidential information and will be dealt with by the Chair of the Steering Group as an act of misconduct.

Breaches of Security

Any breaches of security must be reported immediately to the designated ICT Officer or the Community Worker.

Access to Other Systems and Files

You must not use a Caring Hands in the Vale computer to gain access to any other computer system (hacking). It is only permissible to access or create files or data in areas within the scope of your job description. Files received by email, CD or USB drive, from outside the organisation must be treated with caution to reduce the risk of virus infection.

Removal of ICT Equipment

Approval must be obtained from the ICT Officer or Community Worker before any computer equipment or assets of any description are removed from the premises. This restriction does not apply to laptop computer assigned to individuals, however, individuals will be asked to sign-out transportable ICT equipment such as laptops and will therefore be liable for their upkeep and safe keeping.

Commented [sw1]: Do we need a signing out system?

Remote Access

Any employee or volunteer using remote access to the organisation's servers must abide by the same protocols and guidance as described in this policy.

Passwords and User Identifiers

Passwords and user Identifications will be distributed to staff by the designated ICT Officer for equipment log-in and passwords. These must not be changed without notification of and in agreement with ICT Officer.

Your passwords must be kept confidential, not written down and not disclosed to anyone. Whenever there is a possibility of security being compromised, passwords must not be changed. User identifications must not be shared.

Rights to Monitor and Intercept

Caring Hands in the Vale reserves the right to access all information on its equipment (subject to complying with the Regulation of Investigatory Powers Act 2000 and the Data Protection Act 1998).

Any monitoring of emails, data file or web access containing personal data will be carried out in line with the UK Information Commissioners Draft Code of Practice on the use of personal data in Employer/Employee Relationships.

Internet and Intranet Usage Code of Practice

The organisation provides internet access to enable employees and volunteers to carry out their daily activities.

Caring Hands in the Vale will control access to external websites. Software is able to block certain 'categorised' websites in a more comprehensive manner than previously and will inform any person attempting to access such sites that the site in question is blocked.

Commented [sw2]: We don't at the moment, but we could to some extent

Sites which have been blocked as they are deemed inappropriate to access via the organisations network are listed and available from the ICT Officer. Should access be required to a blocked site for a business purpose, a request must be made via a Senior Manager.

Commented [sw3]: There is no list

All internet access will be automatically recorded and log files reviewed periodically. All detailed reports and logs will be recorded against the User identification. This will be held in a restricted database within the confines of the organisation ICT Officer, and only accessed in the event of a formally approved investigation.

Please note: this monitoring does not capture any data or transactions when a secure area of a site (https) is accessed (i.e., Internet banking login pages), thus ensuring employee privacy.

Commented [sw4]: We can record this information if we want, and some is stored in browser history whci I can accesss. This may include some aspects of online banking by not the passwords etc

The use of Caring Hands in the Vale's systems to receive, view or transmit content that may be considered offensive is expressly prohibited. This will render and employee or volunteer subject to disciplinary action - irrespective of the type of access control implemented.

A secure computer network is available to all our offices and is protected by a firewall from the world-wide network.

Commented [sw5]: There is no formal firewall at present, although there is a firewall on each computer to reduce risks of h acking.

We need to say something about data stored on computers that is confidential. We have to protect this from potential access by other parties.