

## **CWT: IT ACCEPTABLE USE POLICY**

1. This policy regulates all information technology activity involving hardware and software owned by, licensed to, or on the premises of CWT Chamber Training (even if not owned by CWT Chamber Training) in support of its mission.
2. Computers and networks allow access to resources both on and off sites and communication with other users throughout the world. This is a privilege, not a right and requires that individual users respect the rights of other users and the integrity of the systems and associated resources.
3. Users must also observe all relevant UK and European laws and company regulations/policies, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct, data protection, health and safety and computer misuse. Remember, ignorance of the law is no defence.
4. CWT has software and systems in place that can monitor and record all Internet, network and email usage. These security systems record activity for all users.
5. CWT reserves the right to inspect any and all files stored in user areas of its computers, file servers and network, in order to assure compliance with policy. This includes standalone PCs.
6. Misuse of computing, networking or information resources may result in the loss of computing and/or network privileges. Additionally, misuse can be prosecuted under applicable statutes.

Users may be held accountable for their conduct under any applicable company policies, procedures, or collective bargaining agreements. Complaints alleging misuse of IT resources will be directed to those responsible for taking appropriate disciplinary action as specified under CWT's disciplinary policy, illegal copying of software protected by Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment.

7. External organisations operating or providing IT facilities that are accessible from CWT's network may have their own policies governing the use of their resources. Users at CWT are responsible for adhering to both CWT policies and the policies of the external organisation concerned.

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

- Using a computer account that you are not authorised to use. Obtaining or using a password for a computer account which you are not authorised to use. (If you as an authorised user give out your account and password to anyone else, you will be held responsible for the actions of that person.)
- Using CWT's network to gain unauthorised access to any computer systems on or off-site.
- Knowingly or carelessly performing an act which will interfere with the normal operation of computers, terminals, peripherals, network devices or servers.

### ***Prohibited Use***

Users shall NOT use CWT's network or Internet services to view, download, save, receive, or send material related to or including:

- Offensive content of any kind, including pornographic or explicit material
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability
- Threatening or violent behaviour

- Illegal activities
- Commercial messages
- Gambling
- Sports and/or entertainment sites (except as required under the curriculum)
- Personal financial gain
- Forwarding e-mail chain letters
- Sending of unsolicited e-mail (known as spamming) from CWT's sites or company machines
- Material protected under copyright laws
- Sending CWT-sensitive information by e-mail or over the Internet
- Dispersing corporate data to CWT's customers without authorisation
- Opening files received from the Internet without performing a virus scan
- Use of CWT's system in order to misrepresent yourself and CWT to others
- Saving or playing games or unauthorised executable files on the network
- Sending broadcast network messages unless directed to do so by a member of the teaching staff
- Connecting any unauthorised computer to CWT's network without prior permission from the Operations Director
- The use of computer hacking tools may lead to instant dismissal and possible prosecution
- Any interference with the standard "look" of the computer system. This may also lead to disciplinary action to the offender.

Only authorised staff may install or authorise the installation of software to any computer system. Any breach of this instruction will breach licensing agreements and can be dealt with in line with the Disciplinary Procedure.

### **Cyberbullying**

CWT is committed to Safeguarding learners and cyberbullying will be taken very seriously. Cyberbullying may take different forms: threats and intimidation; harassment or "cyber stalking"(e.g. repeatedly sending unwanted texts or instant messages); vilification / defamation; exclusion or peer rejection; impersonation; unauthorized publication of private information or images.

CWT will take steps to identify the person responsible for the bullying. Steps can include looking at the Company's system and computer logs; identifying and interviewing possible witnesses; and, with police involvement, obtaining user information from the service provider. Once the person responsible for the cyberbullying has been identified the Company disciplinary procedure will be followed.