

THE USE OF IT EQUIPMENT PROVIDED FROM BRANCH FUNDS

Computer and telephony equipment purchased using UNISON funds should be used only for UNISON purposes, and for activities in line with UNISON's rules, aims and policies, including political activity. The branch must ensure that controls are in place to make certain that this equipment is used only for these purposes, and not used in activities contrary to UNISON rules or aims, or contrary to the furtherance of its policies.

Branches must ensure that branch officers who are allocated equipment to assist them in their union duties comply with these guidelines at all times, and that any such equipment is returned to the branch at the end of their period of office (Rule G.4.2.5.).

The Computer Misuse Act, 1990 provides a legislative framework within which all branches must work.

What is computer misuse?

Misuse of computers and communications systems can take several forms:

1. Data misuse and unauthorised transfer or copying
Copying and illegal transfer of data can be very easy using large storage devices such as hard drives, CDs and USB pen drives. Any kind of data can be copied all too easily and without permission if the branch does not have secure processes in place.
2. Copying and distributing software, music and film
This includes copying music CDs with computer equipment, making copies of music tracks and distributing them on the Internet. This is a widespread misuse of both computers and the Internet that breaks copyright regulations.
3. Pornography
A lot of offensive material is available through the Internet and can be stored in electronic form. Viewing or downloading child pornography is illegal, as is distributing any form of pornography.
4. Hacking
Hacking is where an unauthorised person uses a network, Internet or modem connection to gain access past security passwords or other

security to see data stored on another computer. Hackers sometimes use software hacking tools and often target particular sites on the Internet

5. Identity and financial abuses

This includes misuse of stolen or fictional credit card numbers to obtain goods or services on the Internet, and use of computers in financial frauds. These can range from complex well thought out deceptions to simple uses such as printing counterfeit money with colour printers

6. Viruses

Viruses are programs written by people and designed to cause nuisance or damage to computers and their files

Legal requirements

Listed below are key areas relating to the Computer Misuse Act which branches need to comply with to ensure that branches are operating within the law when using computers:

- a) computer network and application ID and passwords should only be used by the person to whom they have been allocated

The following are all unlawful under the Computer Misuse Act, and could lead to criminal or civil charges. Branches should put processes in place to guard against such incidents:

- b) outputting, altering, copying or deleting data or a computer program without the proper authority;
- c) downloading pornographic or obscene materials for distribution;
- d) gaining unauthorised access to a computer with another person's ID in order to transmit offensive material;
- e) deliberately deleting or corrupting programs or data – including the introduction of viruses where these result in modification of destruction of data;
- f) unlicensed software;
- g) downloading music which breaches copyright;

For further information, visit:

www.out-law.com for general information on the legal implications of the use of ICT and
www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm for the full text of the Computer Misuse Act

This information note forms part of the Code of Good Branch Practice, and UNISON reserves the right to carry out investigations when any of the above activities are alleged.