



Guidelines for all Computer Users

Access to the Centre network and standalone computers will be provided, but only on the understanding that you agree to follow these guidelines. These guidelines apply to all computer users.

Computer (file). storage areas will be treated as Centre property. The Technical team may look at files and communications to insure that the system is being used responsibly. Users should not expect that their work and emails would always be private. You should also be aware that the Technical team can view your computer screen at any time from anywhere on the network without you knowing about it.

- Users are responsible for good behaviour on the computers.
- Eating, drinking, grooming, and the use of aerosol sprays are not considered to be suitable activities in room. Near a computer they may cause serious damage and are strictly prohibited.
- Please do not spend too long sending/receiving email messages - someone else is usually waiting to use the computer.
- Important work files must be copied to your own floppy disk in case you accidentally damage them or delete them from the network server.
- If a "virus alert" occurs when transferring work files from a floppy disk please inform a member of the technical staff immediately.
- Do not use another person's username/password..
- Do not reveal your password to anyone. If you think someone has learned your password then change it immediately.
- Do not trespass in others' folders, work or files.
- The unauthorised access or use of personal information, contrary to the provisions of the [Data Protection Act 1998](#), is not permitted.
- Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files is not permitted and may be considered a criminal offence under the [Computer Misuse Act 1990](#).
- Programs must not be installed on a computer except by a designated member of staff. Do not bring in programs on a floppy disk or download them from the Internet.
- Games must not be loaded, played or used on any computer unless used for authorised training or teaching purposes. In such circumstances advice should be sought from the Centre Manager.
- The unauthorised copying of software, contrary to the provisions of the [Copyright, Designs & Patents Act 1988](#), is not permitted.
- The installing, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the [Obscene Publications Act 1959/1964](#).
- A computer should not be switched off unless it has completely locked up or is unlikely to be used again that day.
- Always make sure that you have completely logged off the computer before leaving it unattended.
- Please leave the computer and the surroundings as you find them.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on your use of the network and rooms.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.

Adapted from *IT Security & Privacy Guidelines for Users, Lancashire County Council* © 1997



Internet Access

Internet access will be provided for you to conduct research and communicate with others, but only on the understanding that you agree to follow these guidelines. These guidelines apply to both pupils and staff.

General

- Users are responsible for good behaviour on the Internet.
- The Internet is provided for users to conduct genuine research and communicate with others. All the sites you visit are recorded. Remember that access is a privilege, not a right and that access requires responsibility at all times.
- Computer (file) storage areas will be treated as Centre property. Technical staff may look at files and communications to insure that the system is being used responsibly. Users should not expect that their work and emails would always be private.
- You should be aware that the Technical team can view your computer screen at any time from anywhere on the school network without your knowledge.
- During lessons, teachers will guide pupils toward appropriate materials. Outside of lessons, families and tutors bear responsibility for such guidance, as they must also exercise with information sources such as television, telephone, cinema, radio, newspaper, magazine and other potentially offensive media.

The following are not permitted:

- Sending, displaying, accessing or trying to access any obscene or offensive material.
- Using obscene or offensive language. (*Remember that you are a representative of your school/organisation/community on a global public system - never swear, use vulgarities, or any other inappropriate language*).
- Harassing, insulting or attacking others through electronic media.
- Violating copyright laws. (*Never copy and make use of any material without giving credit to the author. By itself such work will be of little value as your own work*).
- Revealing any personal information, the home address or personal phone numbers of yourself or other people.
- Private use of the Internet or email service without advanced permission.
- Use of commercial activities by for-profit institutions.
- Carrying on a private business.

Check with a member of the technical team before:

- Opening unidentified email attachments.

Sanctions

1. Violations of the above rules may result in a temporary or permanent ban on Internet use.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.



CLC Network Security Policy

Due to the wide variety of uses, a number of precautions have to be taken to help ensure that the system is kept available and in full working order:

Supervision

- The use of the network should be supervised as closely as is reasonably possible.
- Normal rules apply, and prohibitions such as eating, drinking, grooming and spraying aerosols are strictly reinforced due to the serious damage that may be caused to the equipment.

Network User Access

- Access to the network is available from any network station during the normal day. The Technical team is responsible for ensuring that the stations in the Centre are turned on and off at the beginning and end of the day respectively. The Centre facilities can be booked through the "The Learning Community" system at reception.
- All users are required to log on with their own username. All users have their own password to allow them to log on, which should not be made available to anyone else.
- Accounts not used within a full academic year will be deleted, including all work saved.
- All network system and administration passwords are recorded and kept in a secure place.
- Time and Internet access spent on the network is continually audited for each user.

File Security

- All users have their own area for storing their work on the network server hard disk (the "my documents" folder). This means that they can access their work from any network station. Pupils from the host school save their work directly onto the Brookfield School server when accessing PCs in the CLC.
- Users do not have access to some station and network drives nor are they able to alter or save files outside their own area (except in the authorised shared topic areas).
- Precautions are taken to reduce the chances of infection by computer viruses via the Internet, email, or floppy disk.
- The system performs an automatic backup of each server hard disk to tape every night. A different tape is used for each night and then reused four weeks later. Occasional backup tapes taken at key points (end-of-term, pre-upgrades, etc). are kept in the safe for longer periods of time before reuse.
- All users should also be encouraged to perform backups of their own files on their own floppy disks.
- Station backups are not required. A faulty station quickly be rebuilt with all the necessary software via files stored centrally on the server.
- The network servers are located in the Technical Office. This office is locked (secure store) when not under direct supervision.

Access to Software

- All users receive desktop icons and start-menu-shortcuts to the main application programs and common utilities.
- Users can only access software and other resources as made available to them. Access to certain resources such as Internet software may also be removed for certain network users, where found to be necessary.
- Sites visited on the Internet are also audited and filtered - see our [Internet Security Policy](#).



Access to Printers

- Printers are available in all activity areas.

Hardware Security

- An inventory of all equipment together with make, model, serial number, date of purchase and location is maintained by the Technical team.
- Items having significant value are registered on a service contract to insure against major repairs.
- Rooms with computers must be locked overnight and when not in use, where possible.
- All rooms and corridors are monitored by the school's alarm system and the Centre's CCTV linked to Knowsley Security after hours.
- All major items are security marked to identify them as the property of the Centre.
- Equipment is security tagged and cable tied to the computer in order to discourage their removal.

Electrical Safety

- All equipment attached to the main electrical supply is safety tested annually.
- The servers operate from an Uninterruptable Power Supply (UPS). to protect against power surges and blackouts.

Fire Protection Measures

- Waste material should be frequently removed from the computer areas.
- A carbon dioxide (CO2). fire extinguisher is required in all main computer rooms and staff should ensure that they know where it is and how to use it.

Internet Security Policy

The Internet is a valuable resource that is freely available to all clients and staff at the Centre. Due to the "unsuitable" nature of some material on the Internet and the possible misuse of email, a number of precautions have to be taken to help ensure that the system is used responsibly:

The use of the Internet will be supervised as closely as is reasonably possible during booked sessions. Technical staff can view a computer screen at any time from anywhere on the school network without the user knowing about it.

- Users are guided onto the Internet via The Centre's Intranet page. This contains links to sites that are relevant and which have been selected by the teachers and KMBC.
- The search engines that are provided as links on our WebPages are only those that make an effort to prevent the inclusion of links to "unsuitable" sites in the listed results of any searches made.
- Access to many, if not most sites considered to contain "unsuitable" material is prevented by a filtering system provided by KMBC.
- Chatlines are not considered to be a suitable use unless used through Schoolmaster. net.
- Precautions are taken to reduce the chances of infection by computer viruses via the Internet or email, which may then be inadvertently taken home on a floppy disk.
- Users found searching for "unsuitable" material or sending offensive email messages will have their access denied for a month and further action taken depending on the nature of the offence. Repeated abuse of the facilities will result in further and more serious action being taken.

Copyright, Designs & Patents Act 1988

The "Copyright, Designs & Patents Act 1988" provides the same rights to authors of computer programs and materials as literary, dramatic and musical authors have to their works. Those rights extend for the life of the author and for fifty years after the author's death. The rights cover; broadcast and public



performance, copying, adapting, issuing, renting and lending copies of videos, DVDs and CDs to the public. Videos/DVDs purchased for home use **should not** be broadcast in the Centre.

Performance and Broadcast of Musical Works

The Performing Rights Society issues licences to cover musical works in broadcasts, cable programmes, online and telephone services. A Public, Performance and Broadcast of musical works licence has been purchased by the Centre to allow music to be played in the CLC at the discretion of the Centre Manager. The necessary hardware to broadcast music is installed in most activity areas.

Section 34(1) of the 1988 Copyright, Designs and Patents Act gives educational institutions the right to record off-air for educational purposes any radio & television broadcasts and cable programmes without infringing copyright. In addition to this, a certified licensing scheme is in place for members of educational institutions.

The ERA License

The Educational Recording Agency license allows members of educational institutions to make recordings of broadcast materials by ERA members (either at work or at home) for bona fide educational purposes. This license includes feature films and advertisements. The ERA license allows:

- Recording, playing back and copying (including transferring from an analogue to a digital medium) of broadcast materials for educational purposes is allowed. These purposes include the delivery of educational objectives to registered students of the educational establishment, but not performances to audiences who pay, or for entertainment, or to promote the institution.
- Extracts from broadcasts can be recorded, compilations of extracts from different programmes can be made, recorded programmes can be edited (as long as the recording is not adapted, e.g. by substituting another soundtrack).
- Copies of recording can be made, as long as they are not sold or hired out.
- Copies can be lent to students provided that they use them only for educational purposes.
- Commercially bought or hired tapes or videos cannot be copied under the terms of the ERA license, it must be the version that was broadcast e.g. on television.
- Recordings made under the ERA license must be labelled with the date and title of each recording, together with the statement "This recording is to be used only under the terms of the ERA License".

Software is generally not sold outright to the purchaser. Instead the purchaser is granted the right to use it as laid down in the user licence. It is normally expected that for a single user licence only one person at a time will have access to and use the software concerned. A network licence may be purchased, normally at a reduced rate, for a defined number of users. A site licence may be available to cover all (unlimited) users within the premises.

It is thus illegal to make copies of software without the copyright owner's consent, or to duplicate software loaded on a hard disk for use on any other personal computer unless allowed for under the licence. Anyone convicted of an offence under this act can expect a fine of unlimited amount plus a prison sentence ranging up to a maximum of 2 years.

Be aware that when copying materials from the Internet, Copyright regulations apply.

Under NO circumstances must any materials which do not comply with copyright regulations be used in Centre literature or resources.