# Adult Community Learning Service Computer Use Policy

## (Including E-Safety, e-responsibility and acceptable use)

### Introduction:

LB Camden Adult Community Learning Service (ACL) uses technology extensively across all areas of the curriculum. Online safeguarding (e-safety) is an area that is constantly evolving and as such, this policy will be reviewed as necessary. We have a duty of care to ensure that all our learners are competent, informed, safe users of ICT and web based resources. Understanding e-safety online is a life skill and we will endeavour  to empower learners to safeguard themselves and their personal information ACL is committed to supporting staff and learners to understand what safe internet use means, to identify and prevent potential risks, and identify and alleviate risky behaviour.

### Our learners and staff are asked to follow these guidelines:

The ACL service encourages users to make effective use of the Internet and the computer network. Such use should always be lawful and appropriate.  It should not compromise the ACL service information and computer systems nor have the potential to damage the Service reputation.

### ACL should maintain a secure Infrastructure:

By Infrastructure ACL mean: computers, mobile devices, physical servers, document storage, Internet filtering, and security patching.

Our entire infrastructure is supported by the Camden Schools IT Support Service (SITSS).  ACL and SITSS are in continuous contact, meetings are held regularly and responses to any e safety issues co-ordinated.

### What are e-safety and e-responsibility?

E-safety and e-responsibility define how we use technology with safety and responsibility in mind. They encompass all internet technologies and electronic communications such as mobile phones, as well as collaborative tools and personal publishing platforms such as Social Networks and blogs.
They highlight the need to educate learners and staff about the benefits and risks of using technology, as well as providing safeguards and awareness for users that allow them to control their online experiences.

### Roles & Responsibilities

ACL will:

1.1. Review this policy annually and in response to any e-safety incident to ensure that the policy is up to date.

1.2 The Safeguarding Officer will:

- Have overall responsibility for e-safety within the service.

- Ensure all aspects of technology within the Service meet the e-safety requirements within this policy.
- Ensure e-safety incidents are properly dealt with and ensure policies and procedures are effective in managing those incidents.
- Delegate the day-to-day management of this to the Digital Infrastructure manager/coordinator with responsibility for e- Safety.

1.3 The Digital Infrastructure manager/coordinator will:

- Keep up to date with emerging risks and threats including sexual exploitation and radicalisation and extremism through technology.
- Inform the Safeguarding Officer in regards to training, identified risks and incidents and advise on changes to the policy.
- Monitor and ensure the effectiveness of e-safety training within the service.
- Recommend further initiatives for e-safety training and awareness within the service.

1.4 Any e-safety incident is reported to the Safeguarding Officer, or the Digital Infrastructure manager/coordinator in her absence or to the Head of Service on the absence of both, and an incident report is made.

1.5 Schools IT Support Service (SITSS) is responsible for ensuring that the ICT technical infrastructure is secure and monitored; this will include ensuring the following:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Operating system updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solution such as internet filtering or monitoring are operating correctly
- Filtering levels are applied appropriately; that categories of use are discussed and agreed with the Safeguarding Officer and the Digital Infrastructure manager/coordinator.

**Note:** Policy regarding the use of personal devices is included in the Tutor's Hand Book.

**Storage of personal documents and photographs on Public drives, tablets and cameras**

Learners should not save personal information and photographs of themselves or others on ICT equipment (including tablets, mobile devices and cameras) or the shared drive used in Camden learning centres. Any personal information or photographs must be deleted by the tutor at the end of a class.

Learners will need to sign a **Storage of personal documents and photos on the Public drive, tablets and cameras disclaimer** at the start of a course where they will be using personal information and photographs has part of their course work. (*Appendix 1*)

**Keeping learners safe:**

There are a number of potential risks to learners when using technology:

- Contact with unsuitable people
- The temptation to meet with strangers
- Exposure to inappropriate content
- Potential for cyber bullying
- Fake profiles
- Too much personal information given out
- Damage to online reputation

**Online safety issues to be aware of**

Mobile phones

- Cyber bullying
- Sexting

Social media

- Privacy settings
- Inappropriate content
- Inappropriate comments
- Paedophiles
- Extremism
- Tagging

Email and internet use

- Privacy
- Phishing
- Viruses
- Fraud
- Copyright
- Online reputation
- Validity and bias

**Understanding the terms**

There are a number of terms used in technology and communications that it is useful to understand.

**Cyberbullying:** abusing someone using technological media

**Sexting:** the act of sending explicit messages or photographs primarily between mobile phones

**Gaming:** engagement in different types of online video games, often shared across different groups of people

**Phishing:** the use of email or SMS in order to obtain personal security information and data

**Privacy settings:** the settings that allow you to ensure that only those who you want to see personal information can do so

**Chatroom:** an interactive online forum which allows people to talk in real-time. The chatroom is the virtual online location where the chat takes place

**Piracy:** illegally copying copyrighted software, music or movies

**Mouse trapping:** A commonly used technique by pornographic sites where a user gets "locked" in a website. While surfing the Internet it is possible to click a website and have multiple undesirable websites open. When this happens, you often cannot close or back out of the sites and must close your Web browser completely

### Use of computer facilities:

The ACL service expects all users to use the Internet and the computer network responsibly and strictly according to the following conditions:

All public computers provide filtered Internet access to help prevent unsuitable use. This is because the council has a duty to

- protect users from accessing sites that may cause offence
- protect vulnerable people
- protect the council network from damage.

A list of the main broad categories is available on request, and includes e.g. chat rooms, drugs, gambling, hate and discrimination, instant messaging, obscene, racist or defamatory material. However, sometimes the filter may block access to sites that seem to have unsuitable content. If you get the message "**access denied**", for a site you consider harmless, please ask a member of staff to contact the helpdesk. They will investigate the site and either unblock it if it has been inappropriately blocked, or they will explain why the site should remain blocked.

This may not be possible immediately, and in some instances may take several days.

### Internet access is monitored:

- Users are advised that staff will monitor Internet access.
- Users accessing sites which do not comply with the conditions of use may be prevented from further use of this service.
- Information gathered on unsuitable use may also be shared with other interested parties e.g. the police.

### Unsuitable use:

Users **must not** change settings or customise computers without staff permission.

Users **must not** access, create, copy, store, transmit or publish any material which:

- is illegal
- is obscene, racist, or defamatory
- would be in breach of copyright
- causes gross offence to, or harassment of, others
- is extremist, provoking hatred or intolerance

**Reporting:**

If inappropriate material is accessed accidentally, users should immediately report this to their tutor. If inappropriate use of the internet or network is discovered or suspected, please tell your tutor immediately without changing the evidence.

**Monitoring:**

The ACL service will monitor the use of the Internet to see whether users are complying with the policy.

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse, images of children, apparently under 16 years old involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK
- terrorist material and publications

There are a number of laws that have a bearing on the use of the ACL service computer facilities, which all users must obey. These include:

a) **The Data Protection Act 1984 and 1998**;

b) **The Computer Misuse Act 1990** these offences are punishable by law with prison sentences ranging from six months to five years and unlimited fines;

c) **The Copyrights, Designs and Patents Act 1988** Users must respect the copyright of all material and software made available by Information Services and third parties. Such material is often obtained by the CLC at special rates, and this arrangement is jeopardised by unauthorised copying. If copyrighted material is to be incorporated into material published online (for example, via the World Wide Web), the permission of the copyright holder must first be obtained;

d) **Obscene Publications Act 1956; Criminal Justice And Public Order Act 1994; Protection Of Children Act 1978** Using computer facilities for the storage, transmission or display of obscene material is illegal. In addition to the serious penalties faced by the offender, investigation may result in confiscation of computer equipment by the police.

e) **Libel Laws** the libel laws cover publishing via electronic media, sending defamatory material via email, or publishing it on the World Wide Web, can lead to prosecution.

## Appendix:

### Storage of personal documents and photos on the Public drive, tablets and cameras.

### Storage:

Learners should not save personal information and photographs of themselves or others on ICT equipment (including tablets and cameras) or the shared Public drive used in Camden learning centres.  Any personal information or photographs should be deleted at the end of a class.

Learning centre ICT equipment and the Public drive is used by other centre users throughout the week.

Learners are responsible for saving work that contains personal detail and photographs to a removable device, typically a memory stick.

### Disclaimer:

Personal Portable digital devices remain the responsibility of the user at all times. Camden Council accepts no responsibility for any loss or damage or problems relating to personal digital devices used in the learning centres.

The Public shared drive is not a private space and Camden Council cannot be responsible for any breeches regarding personal data stored on that drive.

Tablets and cameras will be used by other people and Camden Council cannot be responsible for misuse of any data left on them.

| | | |
|---|---|---|
| **Course:** | | **Venue:** |
| **Term:** | | **Date:** |
| **Print name** | **Signature** | **Date** |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |