Adult Community Learning
Computer Use Policy
(Including e-safety and acceptable use)

Service: Adult Community Learning (ACL) Essex

Title: Adult Community Learning Essex - Computer Use Policy

Control of Document: ACL Senior Management Group

Applies: Whole Service

Policy Aims and Intention:

Safety and security is a prime consideration for all education establishments using the Internet. To ensure we provide a safe learning environment for our users, Adult Community Learning Essex (ACL) adheres to the internet safety policy and systems of its Internet Service Provider (ISP) and the JANET(UK) (Joint Academic NETwork). The systems are deployed to reduce the risks associated with Internet use in an education environment.

Original Date of Acceptance: **December 2011**

Last Review date: **October 2016**

Next Review date: **October 2017**

Introduction

The purpose of this policy is to ensure that ACL Essex users understand the way in which the Internet and the computer network are to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk. The legal framework that informs this policy is included in Appendix 1.

Scope

The policy applies to ACL learners, and staff accessing the teaching and learning network.

ACL staff that have access to the Essex County Council administration network are bound by the policies of the County Council and will be governed by whichever policy is the stronger.

ACL's networks are connected to Internet at each Centre through a common ISP. The Service also uses JANET(UK) for its web services where the JANET(UK) Acceptable Use Policy governs the use of JANET. Further details can be found at http://www.ja.net/documents/publications/policy/aup.pdf

Policy statement

ACL Essex encourages users to make effective use of the Internet and the computer networks. Such use should always be lawful and appropriate. It should not compromise ACL's information and computer systems nor have the potential to damage ACL's reputation.

It is inappropriate use of the internet system for users to access, download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass or intimidate another person. Please note that this also applies to use of social media systems accessed from ACL systems.

Use of computer facilities

For the purposes of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups.

ACL Essex will promote safe and responsible use of the internet through 'Guidance for Internet Safety' (appendix 3) and publicising acceptable and unacceptable use.

ACL Essex expects all users to use the Internet and the computer networks responsibly and strictly according to the following conditions:

Acceptable Use:

You must:

1. Use these computers and the internet for work and tasks that support learning and achievement on your course.
2. Always log off properly when you have finished and leave the equipment as you would expect to find it.
3. Make sure e-mails are polite and courteous.
4. Make sure you know what 'unacceptable use' is and immediately report unacceptable use to a member of staff.
5. Store work on the VLE (Virtual Learning Environment) or shared file areas provided. Leaving work on individual computers is not protected.

Unacceptable use:

You must not:

1. Attempt to install or store any programmes or games onto the computer system.
2. Dismantle; damage, disable or remove parts from computers or network equipment (e.g. mouse, keyboard, cables).
3. Attempt to connect your own personal laptop, PDA or any other device via cable, wireless, or any other means to the system.
4. Attempt to repair faults.
5. Change the settings on the computer – including screensavers, internet or network settings, defaults and e-mail settings.
6. Use ACL systems for commercial purposes (buying and selling).
7. Change or destroy other people's information or files.
8. Upload, download, or otherwise transmit (make, produce or distribute) shareware/software or any copyrighted materials.

9. Breach copyright law relating to computer software, music, video or other copyrighted material.
10. Copy information to submit as your own on externally accredited programmes (plagiarism).
11. Use ACL equipment for the production or publication of printed material that is not explicitly course related.
12. Intentionally waste resources (e.g. excessive printing, unnecessary e-mails). Print runs of more than 20 pages must be agreed in advance with a member of ACL staff.
13. Eat or drink near computer equipment.
14. Ignore any ‘Virus Detected’ message, or fail to act on the instructions within it.
15. Engage in ‘Chat’ or ‘Chat room’ activities on the Internet, unless this is a part of your course.
16. Arrange to meet anyone over the Internet.
17. Access, download, store or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass or intimidate another person. Please note that this also applies to use of social media systems accessed from ACL systems.
18. Send or forward spam, chain, junk or nuisance e-mails.
19. Open e-mail attachments unless you know it is from a reliable source.
20. Attempt to guess other user’s passwords, bypass security in place, hack into, or alter settings on computers or the network or gain access to areas of the system for which you do not have the appropriate permissions.
21. Publicise or transmit personal or confidential information.
22. Use any hacking or key/code cracking software, or attach additional devices to the network.
23. Disclose your password to others or use passwords intended for others. Users are responsible for all actions performed using their ID.
24. Intentionally interfere with the normal operation of the Internet connection, including introducing computer viruses or any other malicious computer code/programs, sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion and hinders others in their use of the Internet.
25. Tick boxes to “remember me on this computer” or remember password for future logins.

ACL acknowledges that in certain planned learning activities, access to sites which may seem inappropriate, may be beneficial for educational use (for example investigating racial issues). Any such access should be pre-planned and recorded so that it can be justified if required.

Reporting

If inappropriate material is accessed accidentally, users should immediately report this to a member of staff so that our IT staff can be informed. If inappropriate use of the internet or network is discovered or suspected, please tell a member of staff immediately without changing the evidence. There are posters in the classroom advising how to contact and report an incident. There is also a link on the home page of the VLE: http://moodle.essexacl.ac.uk where you can find details of how to report an incident.

Appendix 2 shows the reporting process. This process should be strictly followed to ensure the appropriate actions are carried out.

Monitoring

ACL will monitor and audit 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 and extremist material

If a user’s conduct and/or action(s) are illegal, the user may become personally liable.

Any other potential misuse identified by ACL will be reported and will lead to the Personal Responsibility Procedures (learners), or Misconduct Procedures (staff) being applied.

Appendix 1 - Legal Framework

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

a) The Data Protection Act 1984 and 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents

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 http://www.legislation.gov.uk/ukpga/1990/18/contents

c) The Copyrights, Designs And Patents Act 1988 Users must respect the copyright of all material and software made available internally and by third parties. Such material is often obtained by the Service 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 http://www.legislation.gov.uk/ukpga/1988/48/contents

d) Obscene Publications Act 1959 http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents; Criminal Justice And Public Order Act 1994 http://www.legislation.gov.uk/ukpga/1994/33/contents; Protection Of Children Act 1978 http://www.legislation.gov.uk/ukpga/1978/37/contents 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 expensive prosecution.

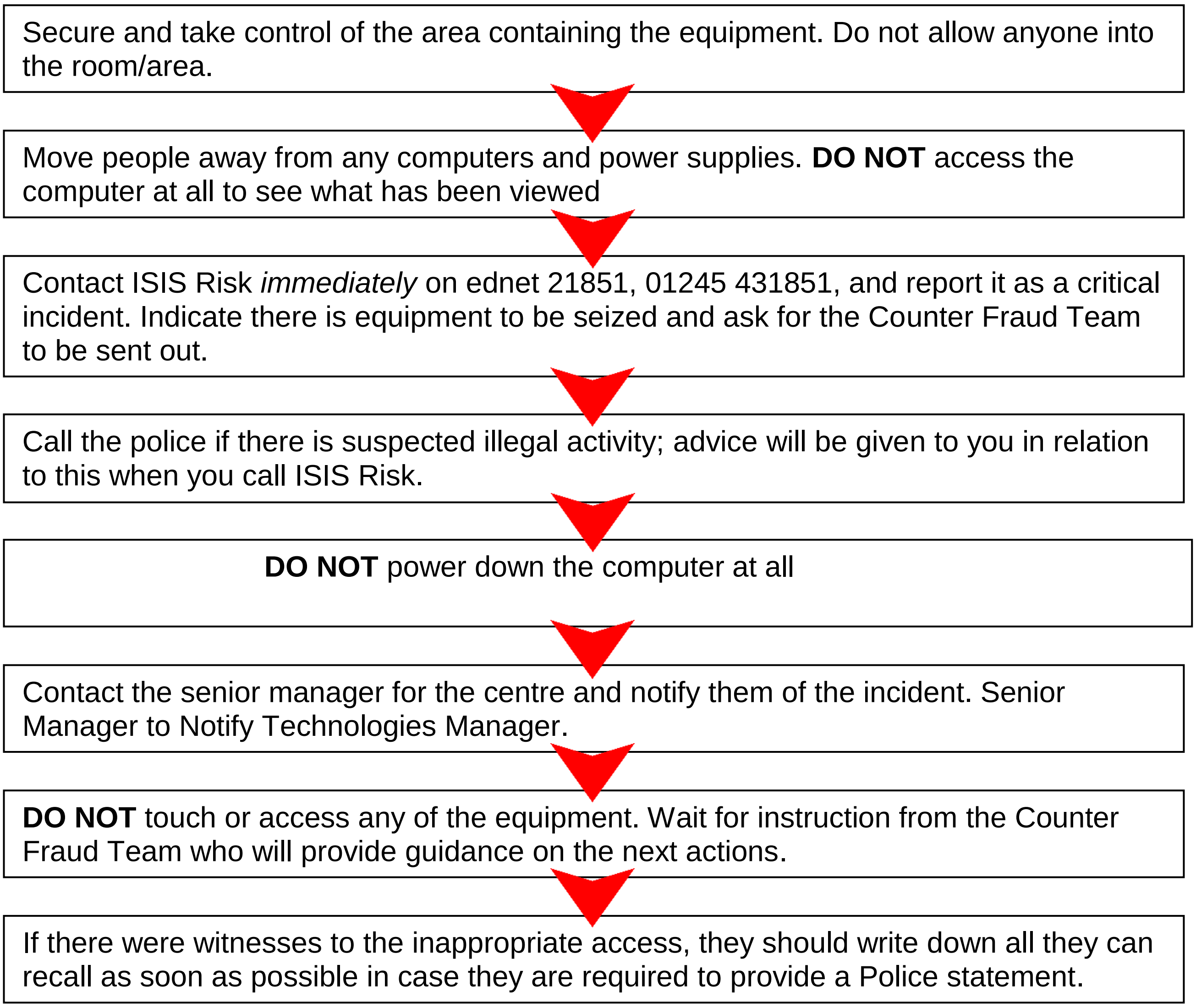
f) The Prevent Duty Guidance for higher education institutions in England and Wales – Departmental advice for schools July 2015 – linked to the Counter-Terrorism and Security Act 2015 – related to having due regard to the need to prevent people from being drawn into terrorism. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

Appendix 2 - Internet Safety Protocol

The following Internet Safety Protocol is designed to be followed in the event that the Internet is used to access (or if there is suspicion of access) inappropriate or illegal material.

As these situations only occur rarely, this flow diagram is provided to give quick and easy guidance about what to do. ACL may be required to provide supporting information in this type of situation. As a result of the legal position, ACL has internal processes and procedures in place that enables information to be provided swiftly whilst adhering to relevant laws. This process may also help to defuse the tension that can be associated with these situations. Be assured that ACL will manage any such situation both in, and with, confidence.

Initial Steps:



Secure and take control of the area containing the equipment. Do not allow anyone into the room/area.

Move people away from any computers and power supplies. **DO NOT** access the computer at all to see what has been viewed

Contact ISIS Risk *immediately* on ednet 21851, 01245 431851, and report it as a critical incident. Indicate there is equipment to be seized and ask for the Counter Fraud Team to be sent out.

Call the police if there is suspected illegal activity; advice will be given to you in relation to this when you call ISIS Risk.

DO NOT power down the computer at all

Contact the senior manager for the centre and notify them of the incident. Senior Manager to Notify Technologies Manager.

DO NOT touch or access any of the equipment. Wait for instruction from the Counter Fraud Team who will provide guidance on the next actions.

If there were witnesses to the inappropriate access, they should write down all they can recall as soon as possible in case they are required to provide a Police statement.

Appendix 3 - Guidance for Internet Safety

To protect yourself and your computer against online threats

1. Get security software with **anti-virus**, **anti-spyware** and a **firewall** and keep these up to date.
2. Use an up to date **web browser** that will warn you against known harmful websites.
3. Make sure **passwords** have a mix of several words, letters, numbers and punctuation, and use different passwords for different sites
4. **Avoid** easy passwords like – **'123456'**; '**password'**; **'letmein'**; **'monkey'**; **'qwerty'**; '**abc123'**
5. Never reply to **spam**, not even to try to unsubscribe.
6. Make sure you know how your personal details will be used before giving them to companies
7. Protect yourself against eavesdroppers and freeloaders by **encrypting** your wireless network.

When using blogs, chat rooms and social network sites (e.g. MySpace, FaceBook or Bebo)

8. When registering with social network site always check you can unsubscribe if you need to.
9. Use a nick-name and do not tell people your address or telephone number.
10. Be careful about who you accept into your group of friends. These people can see your details.
11. Think about what you post on the internet before you do it. It will be on the net forever.
12. Do not meet up with someone that you have been chatting to on the internet. If you do, always take a friend with you for the whole meeting.
13. Make sure you know how to report abuse or bullying on the site and how your complaint will be dealt with.
14. For protecting your personal information, check the advice on web sites like https://ico.org.uk

For On-line shopping and auctions

15. Visit 'Get safe online' before you shop online or use online auctions https://www.getsafeonline.org
16. When paying on line, make sure the URL (address) of the payment page starts https:// rather than http:// and look for a closed padlock symbol when paying for goods online. This is a sign the page is secure to take payments.