

Bournemouth Adult Learning Computer Use Policy (including e-safety and acceptable use)

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, Bournemouth Adult Learning (BAL) adheres to the internet safety policy and systems of its internet service provider (UKERNA). The systems are deployed to reduce the risks associated with Internet use in an education environment.

Introduction

The purpose of this policy is to ensure that Bournemouth Adult Learning users understand the way in which the Internet and the computer network is 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 BAL learners, and staff accessing the curriculum network. BAL staff who have access to the Borough of Bournemouth administration network are bound by the policies of the Borough of Bournemouth and will be governed by whichever policy is the stronger.

BAL's network is connected to JANET, and hence the internet. The JANET 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

BAL 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 BAL's information and computer systems nor have the potential to damage BAL's reputation.

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.

BAL will promote safe and responsible use of the internet through Top Tips (appendix 3) and publicising acceptable and unacceptable use.

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

Acceptable Use

Please:

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 is 'unacceptable use' and immediately report unacceptable use to a member of staff.
5. Store work on the VLE rather than on the shared files area (saving resources).

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 BAL 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 BAL 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 BAL 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. Visit inappropriate sites, or download inappropriate material, such as those that may contain pornographic, violent, racist, hacking, illegal or offensive materials.
18. Send, forward or store materials that contain pornographic, violent, racist, hacking, illegal or offensive materials or contain bullying, threatening, offensive or insulting language (cyber bullying).
19. Send or forward spam, chain, junk or nuisance e-mails.
20. Open e-mail attachments unless you know it is from a reliable source.
21. 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 they do not have the appropriate permissions.
22. Publicise or transmit personal or confidential information.
23. Use any hacking or key/code cracking software, or attach additional devices to the network.
24. Disclose your password to others or use passwords intended for others. Users are responsible for all actions performed using their ID.
25. 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.
26. Tick boxes to "remember me on this computer" or remember password for future logins.

BAL 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 the ICT Facilitator 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.

Appendix 2 shows the reporting process. The Quality Manger will be informed so that this can be taken into account in monitoring of this policy.

Monitoring

BAL 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

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

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

The current policy not to issue individual learner logins will be reviewed following incidents of misuse of the curriculum network.

Appendix 1

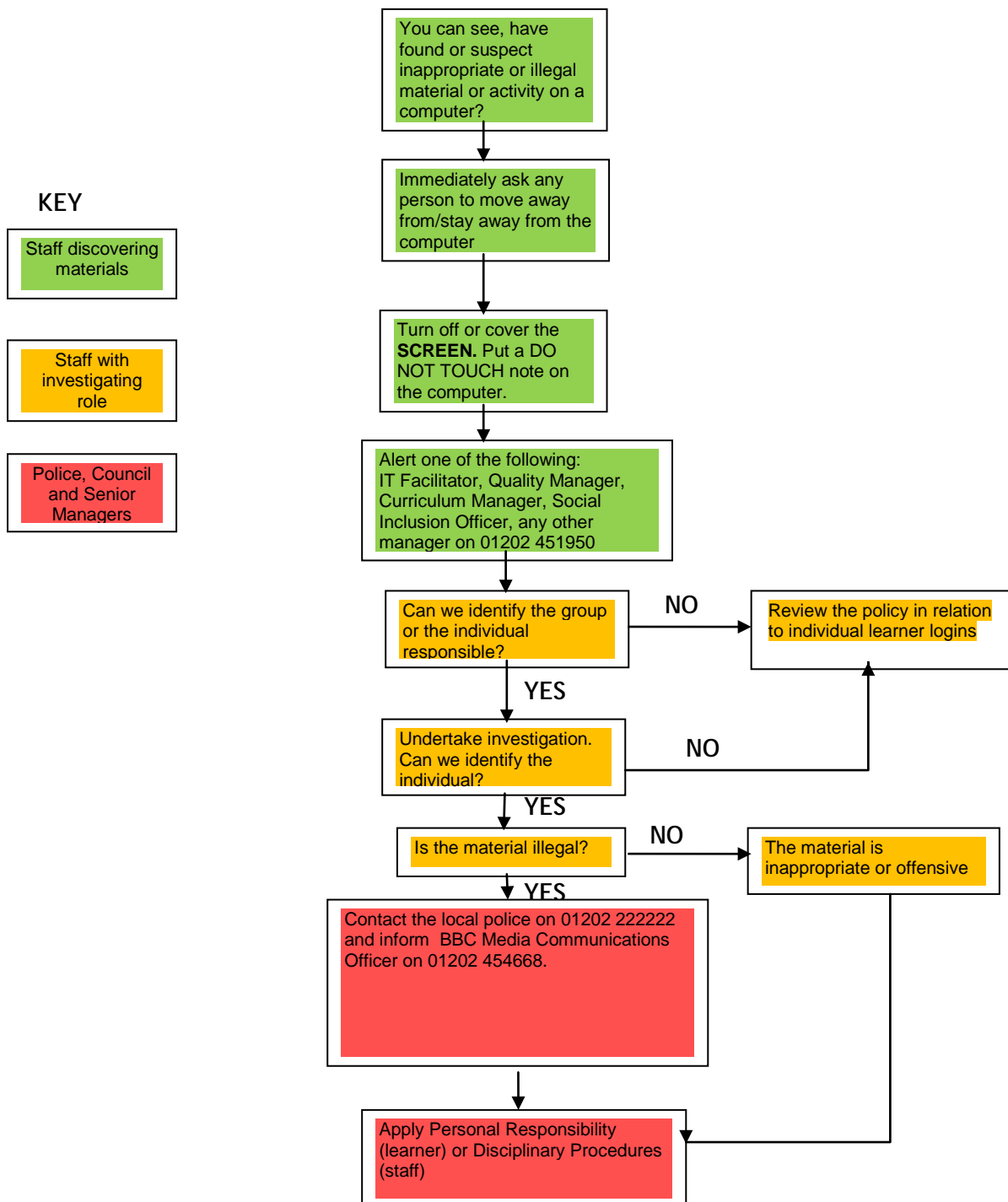
LEGAL FRAMEWORK

There are a number of laws that have a bearing on the use of the BAL's 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 College 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 expensive prosecution.

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 suspicion of access) inappropriate or illegal material. As these situations only occur rarely, when they do arise, this compounds the issue and often leads to a stressful time. This flow diagram is aimed at providing quick and easy guidance about what to do. BAL may be required to provide supporting information in this type of situation. As a result of the legal position, BAL has internal processes and procedures that will bring structure that enables information to be provided swiftly whilst adhering to relevant laws. This structure may also help to defuse the tension that can be associated with these situations. Be assured that BAL will manage any such situation both in, and with, confidence.



Appendix 3

Top tips for Internet Safety

These top tips have been developed following consultation with staff and learners.

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'; 'iloveyou'; 'princess'; 'rockyou'; 'abc123' Never reply to **spam**, not even to try to unsubscribe.
5. Make sure you know how your personal details will be used before giving them to companies
6. Protect yourself against eavesdroppers and freeloaders by **encrypting** your wireless network.

When using Blogs, Chat rooms and social network sites (MySpace, FaceBook or Bebo)

7. When registering with social network site always check you can unsubscribe if you need to.
8. Use a nick-name and do not tell people your address or telephone number.
9. Be careful about who you accept into your group of friends. These people can see your details.
10. Think about what you post on the internet before you do it. It will be on the net forever
11. 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.
12. Make sure you know how to report abuse or bullying on the site and how your complaint will be dealt with.
13. [Check the advice on websites like www.ico.gov.uk/Youth.aspx](http://www.ico.gov.uk/Youth.aspx)

For On-line shopping and auctions

14. [Check the advice at www.getsafeonline.gov.uk](http://www.getsafeonline.gov.uk) before you shop online or use [online auctions](#).
15. 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