

IT ACCEPTABLE USE POLICY

1. This policy regulates all information technology activity involving hardware and software owned by, licensed to, or on the premises of Barry College (even if not owned by the College) in support of its mission.
2. Computers and networks allow access to resources both on and off the College sites and communication with other users throughout the world. This is a privilege, not a right and requires that individual users respect the rights of other users and the integrity of the systems and associated resources.
3. Users must also observe all relevant UK and European laws and College regulations/policies, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct, data protection, health and safety and computer misuse. Remember, ignorance of the law is no defence.
4. The College has software and systems in place that can monitor and record all Internet, network and email usage. These security systems record activity for all users.
5. The College reserves the right to inspect any and all files stored in user areas of its computers, file servers and network, in order to assure compliance with policy. This includes standalone PCs.
6. Misuse of computing, networking or information resources may result in the loss of computing and/or network privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable College policies, procedures, or collective bargaining agreements. Complaints alleging misuse of IT resources will be directed to those responsible for taking appropriate disciplinary action as specified under the College disciplinary policy, illegal copying of software protected by Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment.
7. External organisations operating or providing IT facilities that are accessible from the College network may have their own policies governing the use of their resources. Users at Barry College are responsible for adhering to both the College policies and the policies of the external organisation concerned. Users attention is particularly drawn to the JANET Acceptable Use Policy @ <http://www.ja.net/company/policies/aup.html>
8. Examples of misuse include, but are not limited to, the following:
 - Using a computer account that you are not authorised to use. Obtaining or using a password for a computer account which you are not authorised to use. (If you as an authorised user give out your account and password to anyone else, you will be held responsible for the actions of that person.)
 - Using the College network to gain unauthorised access to any computer systems on or off-site.
 - Knowingly or carelessly performing an act which will interfere with the normal operation of computers, terminals, peripherals, network devices or servers.

APPROVED BY: IS Strategy Group
ISSUE DATE: September 2002
REVIEW DUE: September 2010

ISSUED BY: IS Manager
REVISED: (2) 25 April 2008

This document may be out of date if printed. Up-to-date procedures are available from the Staff Intranet.

- Installing any software, on any College computers, without the knowledge and permission of the IS Manager or his representative.
 - Violating terms of software licensing agreements or copyright laws.
 - Deliberately wasting/overloading computing resources.
 - Accessing or making available any information which is illegal or could be considered to be offensive or inappropriate or is not relevant to a student's studies or staff defined job.
 - Using electronic mail Inappropriately.
8. Activities will not be considered misuse when authorised in writing by appropriate College authorities for legitimate teaching, research, security or performance testing.
 9. Minor infringements of this policy, such as accessing non relevant websites during working/learning time, excessive disk space consumption etc., will normally be dealt with in an informal manner by the appropriate staff [tutor/line manager]. Serious infringements, or repeated failure to comply with the College policies [as sharing accounts or passwords, or repeated minor infringements as described in, but not limited to, the above], will be dealt with formally via College disciplinary procedures and the temporary or permanent loss or modification of IT access privileges. Additionally, where the infringement constitutes an illegal act the appropriate authorities will be informed.
 10. Offences which are in violation of UK laws will result in the immediate loss of all IT and computing privileges, and will be reported to the offender's relevant line manager and the Police.
 11. Any software or files downloaded via the Internet into the College network become the property of the College. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. The College Software Acquisition Policy applies and no software should be installed by a user without prior consultation with the Computer Services Department.
 12. No user may use College facilities knowingly to download or distribute pirated software or data.
 13. No user may use College facilities to deliberately propagate any virus, worm, Trojan horse, Spyware, trapdoor programme code or other malicious software.
 14. Each user using the network facilities of the College shall identify himself or herself honestly, accurately and completely.
 15. No users are authorised to communicate with the media or any public forum in the name of the College. Users may participate in newsgroups or chat rooms in the course of business when relevant to their duties or studies, but do so as individuals speaking only for themselves.

APPROVED BY: IS Strategy Group
ISSUE DATE: September 2002
REVIEW DUE: September 2010

ISSUED BY: IS Manager
REVISED: (2) 25 April 2008

This document may be out of date if printed. Up-to-date procedures are available from the Staff Intranet.

16. The College retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any user in the normal course of the user's work for the College. It is not intended that this apply to the user's personal homepages, etc. accessed from College facilities in free time.
17. Users may use Internet facilities for general browsing during breaks, or outside of working hours, provided that all College policies are adhered to and this use does not cause problems for other users; it should be noted that it is not provided by right or as a general leisure resource.
18. The College will comply with reasonable official requests from law enforcement and regulatory agencies for logs, diaries and archives on a user's network activities; provided the appropriate, correctly completed, documentation is proffered.
19. Users with Internet access must take particular care to understand the copyright, trademark, libel, slander and public speech control laws of all countries in which this College maintains a business presence, so that use of the Internet does not inadvertently violate any laws which might be enforceable against the College or the user.
20. The College has installed a variety of firewalls, proxies, internet address screening programmes and other security systems to assure the safety and security of the College's networks. Any attempt to disable, defeat or circumvent any College security facility is grounds for disciplinary action.
21. Only those Internet services and functions which support College activities will be enabled at the Internet firewall. It is the College's intention that the firewall shall err on the side of caution. This may block many innocent sites initially. Any site that has been blocked but can be shown to have a genuine value to users can be unblocked.

All staff and students using College ICT facilities will be provided with a copy of this policy. All users must sign the following statement:

"I have received a written copy of Barry College's Acceptable Use Policy. I fully understand the terms of this policy and agree to abide by them. I realise that the College's security systems will record the Internet address of any site that I visit and records will be kept of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive may be recorded and stored in an archive file for management use. I also understand that the College reserves the right to inspect any stored files or data downloaded or transmitted. I understand that any violation of this policy could lead to disciplinary action or even criminal prosecution."

APPROVED BY: IS Strategy Group
ISSUE DATE: September 2002
REVIEW DUE: September 2010

ISSUED BY: IS Manager
REVISED: (2) 25 April 2008

This document may be out of date if printed. Up-to-date procedures are available from the Staff Intranet.

This policy at Barry College sits alongside other policies such as the College Charter, Disability Statement, Equal Opportunities Policy, Health & Safety Policy and Child Protection Policy. It also takes into account relevant legislation that includes Race Relations (Amendment) Act 2000, the Disability Discrimination Act (1995) as amended 2001, the Children Act 1989, the Sex Discrimination Act 1975 and the 1974 Health and Safety at Work Act.

APPROVED BY: IS Strategy Group
ISSUE DATE: September 2002
REVIEW DUE: September 2010

ISSUED BY: IS Manager
REVISED: (2) 25 April 2008

This document may be out of date if printed. Up-to-date procedures are available from the Staff Intranet.