BRIDGEND COLLEGE

ITSS004

STUDENT COMPUTER

ACCEPTABLE USE POLICY

Master Copy Control:

Document Author:

Nerys Gimblett Date:
Director of IT, Digital Development and Marketing Services

Document Review:

Chris Long Date:
Health, Safety and Sustainable Development Manager

Andrew Gibbs Date:
Vice Principal Resources

Final Document Review and Approval:

Simon Pirotte Date:
Principal/CEO

1. Introduction

The purpose of this policy is to define a framework on how to best protect the college's computer systems, network and all data contained within, or accessible on or via these computer systems from al threats whether internal, external, deliberate or accidental.

IT Systems play a major part in the College. The availability, confidentiality and the integrity of data on the College IT Systems is critical to the success of our academic and administrative activities. Effective security is achieved with discipline, in compliance with legislation and adherence to College Codes of Practice.

It is the Policy of the College to ensure that:-

- All central computer systems, programs, data and network will be adequately protected against loss, abuse or unauthorised access.
- All members of the College are aware that is it their responsibility to adhere to this policy.
- All regulatory and legislative requirements regarding computer security and information confidentiality and integrity will be met by IT Support Services and the College.
- Create across the college awareness that appropriate measures must be implemented as part of an effective operation of IT Security.
- Ensure all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

The Policy applies to all Students of the College.

2. Responsibilities

The Computer Acceptable Usage Policy sets out the responsibilities for ensuring that all students are aware and adhere to the information provided.

2.1 The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of IT Support Services.

2.2 The College Senior Management Team is responsible for approving the Computer Acceptable Usage Policy and for ensuring it is available for all learners to access.

2.3 All students are responsible for the immediate reporting of any IT incidents to the IT Services Department. The Manager responsible for the department will co-ordinate investigations into any reported IT security incidents.

2.4 The College auditors will periodically review the adequacy of IT systems controls as well as compliance with such controls.

3. The Policy

The College has an obligation to abide by all UK legislation and relevant legislation of the European Community. Of particular relevance are the following:-

- Regulation of Investigatory Powers Act 2000 (RIPA)
- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000.
- The Data Protection Act 1998.
- The Human Rights Act 1998
- The Copyright, Designs and Patents Act 1988.
- The Computer Misuse Act 1990.
- Freedom of Information Act 2000.

3.1. General Computer Usage

3.1.1 All use of the Janet network must conform to the Janet Acceptable Use Policy. Copies are available on the portal.
3.1.2 Students should not access the network without authorisation.
3.1.3 Students should not disclose passwords or authorisations to other individuals either within or outside the College. For reasons of security your individual password should not be printed, stored on-line or given to others. Use of e-mail and the Internet is primarily for college-related purposes.
3.1.4 The College has the ability to monitor e-mail and internet usage and all students should be aware that their use is not private.
3.1.5 Computers and e-mail accounts are the property of Bridgend College and are designed to assist in the performance of your learning. You should, therefore, have no expectation of privacy in any e-mail sent or received, whether it is of a college or personal nature.
3.1.6 Students of the College should conform to common conventions of “Netiquette”. Further information regarding “Netiquette” can be found using the following URL :- http://www.albion.com/netiquette/
3.1.7 It is inappropriate use of e-mail and the Internet if students access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory. You should be aware that such material may also be contained in jokes sent by e-mail. Such misuse of electronic systems will be deemed as misconduct and will, in certain circumstances, be treated by the College as gross

misconduct within the Student Code of Conduct. The College reserves the right to use the content of any e-mail in any disciplinary process.

3.1.8 In addition, the College wishes to make you aware that Closed Circuit Television (CCTV) is in operation for the protection of employees and students.

3.1.9 The College also wishes for you to aware that internet monitoring is in place for both students and staff and should any misuse or concerns arise an investigation will begin.

3.1.10 There are occasions where IT Support Services, on the instruction of the Principal or another member of the Senior Management Team will need to access your individual email accounts, or any relevant drives.

3.1.11 Data on the College network should not be downloaded onto removable storage. No sensitive or personal information relating to staff or students should be downloaded and put onto an asset not owned by the college. Please refer to the College Data Protection Act for further information.

3.1.11 Any removable media that does contains any sort of college data must be locked away is a secure place.

3.1.12 Students should ensure that they adhere to the College's procedures on the Data Protection Act and Freedom of Information Act, copies of which are available on Moodle.

3.1.13 Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or make use of those systems unless authorised to do so. You should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

3.1.14 The IT Support Services Department are there to assist you. If you require any information or help about the use or set up of your computer you should contact them via the helpdesk (ext 373 or via email).

3.2 Use of e-mail

3.2.1 E-mails should be drafted with care. Due to the information nature of e-mail, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from your computer.

3.2.2 Students should not make derogatory remarks in e-mails about employees, students, competitors or any other person. **Any written derogatory remark may constitute libel.**

3.2.3 Try not to create e-mail congestion by sending trivial messages. Students should regularly delete unnecessary e-mails to ensure that disk storage is not wasted.

3.2.4 Make hard copies of e-mails which you need to retain for historical purposes or alternatively archive these. If you require assistance with archiving, please contact the helpdesk.

3.2.5 You may want to obtain e-mail confirmation of receipt of important messages. You should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, telephone the intended recipient to confirm receipt of important messages.
3.2.6 E-mail distribution list should not be used for personal messages such as articles for sale.
3.2.7 Excessive private use of the e-mail system during ke learning times may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.
3.2.11 Do not open emails received from unrecognised sources. In such cases, delete the email without opening it or contact the IT Support Helpdesk for advice on how proceed.
3.2.12 Any emails of a private, sensitive or confidential nature should be marked accordingly when transmitting to third parties.
3.2.13 Email attachments containing sensitive or confidential information should be password protected when sending to third parties. Use of such passwords can be done via communications between the College and third parties to ensure security of this information.

3.3 Use of the Internet

3.3.1 Private use of the Internet is permitted outside of teaching and learning times. Private access to the Internet during contact time may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.
3.3.2 The sites accessed by you must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.
3.3.3 Security threats and inappropriate sites include pages that contain material promoting radicalisation or extremist websites and pornographic images, sites that download copyrighted materials, exposure to inappropriate advertising online gambling, any sites relating to safeguarding issues such as grooming (children or vulnerable adults) and other illegal activities.
3.3.4 Inbound and outbound internet traffic is scanned for security threats and access to inappropriate sites. Access to categories of websites that are deemed unacceptable are blocked by the IT department. Some learners may be involved in legitimate research that involves a blocked website. When this is the case, access should be requested via the IT Helpdesk.
3.3.5 Investigations will commence where reasonable suspicion exists of a breach of this or any other relevant policy. Any suspected breach of this policy must be reported immediately to the Director of IT Manager to allow investigation of the incident prior to taking appropriate action. A suspected breach should not be reported through the IT Helpdesk.

3.3.3 The use of Social Networking sites is permitted, and only deemed ***"Acceptable"*** if used for the purpose of the curriculum and research. Any actions resulting in deformation of the College name and reputation, or malice towards any individual WILL be treated as gross misconduct.
3.3.4 The use of Proxy Avoidance tools/websites is ***NOT*** permitted. **ALL web traffic MUST** pass through the College Web Filtering solution to ensure security compliance with the Janet regulations who provide, monitor and regulate the College network connection to the internet. Any attempts to by-pass the College web filtering system will result in loss of access to the College systems and further action may be taken against individuals.

3.4 Copyright and Downloading

3.4.1 Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.
3.4.2 Copyrighted software must never be downloaded. Such copyrighted software will include screen-savers.
3.4.3 The downloading of bit-mapped images and multimedia files is restricted to the disk space limitation above.
3.4.4 Students should not import non-text files or unknown messages on to the College' system without having them scanned for viruses.
3.4.5 Students should not engage in political discussions through outside newsgroups using the College's computer system.

3.5 Printing and Photocopying

3.5.1 Use of the College Printing and Photocopying facilities is controlled by secure swipe card terminals. Photocopying and Printing facilities are not accessible to students who do not have an ID.
3.5.2 Student ID cards must not be loaned out to other members of staff or students as this could lead to fraudulent use.
3.5.3 Students are responsible for ensuring that information printed or copied must be removed immediately from the printer/copier once the job has been released. The college adopts a "follow me print" policy that allows print jobs to be released at any device on any campus. These print jobs are held centrally on a print server and print queues are purged on jobs older than 3 days.

3.5.4 Photocopying should always be kept to a minimum where appropriate.

4. Document Review

This policy will be reviewed on an annual basis

5. Related Documents

- College Data Protection Policy
- IT Security Policy
- Janet Acceptable Usage Policy
- Email Policy
- Prevent Policy