East Durham College

Policy Document

Policy Number	6.4
Policy Grouping	Security, Confidentiality & Information
Policy Document Title	Computer Usage Policy
Author / Reviser / Owner	Andrew Barker
Date of Current Version	20/09/2017
Review Date	**September 2020**

Impact Assessed	Yes ☒	No □

Approved By	Committee	Date
CMG	College Management Group	18.10.17

Document Control

This document is issued and controlled by Quality & Standards and may only be modified by the designated group after proposed modifications have been accepted by the College Management Group

The latest version of the procedure will be maintained on the College Extranet

Policy Document 6.4
Computer Usage Policy

Scope

This policy concerns all computer systems and network facilities operated at East Durham College. Systems are provided for the use of enrolled students, faculty and staff in support of the College. All computer users are responsible for using the facilities in an effective, efficient, ethical and lawful manner. The College views the use of computer facilities as a privilege, not a right, and seeks to protect legitimate computer users by imposing sanctions on those who abuse the privilege.

Purpose

The Policy applies to all users of the computing and network facilities. Violations of any of the conditions are considered unethical and possibly unlawful. An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the appropriate Curriculum Manager, Director or Principal.

Policy Statement

Computer users agree to use facilities and accounts for College related activities only

Accounts are considered the property of the College. All access to computer facilities, including the issuing of passwords, must be first approved through the Network Administrator and authorisation for the use of the accounts is given for specific academic purposes. Attempts to use accounts without authorisation or to use accounts for other than their intended purposes are all violations of this rule. Loopholes in computer security systems or knowledge of a special password should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorisation has not been given.

East Durham College has a duty of care to filter all web content to ensure its users are protected against unsuitable content including but not limited to adult material, gambling, drugs, offensive, hate, discrimination, racism, violence, terrorism, and extremism, attempting to access or bypass filtering to access this content will be deemed as unacceptable use for which users will be subject to College disciplinary procedures and possible escalation to the police.

Any attempt to overcome the security systems of any College machine is strictly prohibited. Technical Services reserves the right to disable an account if any misuse is determined. Computer equipment and accounts are to be used only for the purpose for which they are assigned and are not to be used for commercial purposes or non-college related activities such as running a word processing service. Game playing is not allowed on any system, unless authorisation is obtained.

An account assigned to an individual, by the College, must not be used by others without explicit permission from the owner of the account. The account owner is responsible for proper password protection. Programs and files are considered confidential unless they have explicitly been made available to other individuals. The Network Administrator may access files when necessary for the maintenance of

central computer systems. When performing maintenance, every effort is made to insure the privacy of a user's files.
Electronic Communications facilities, such as email are for college related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.

Computer users agree to respect the integrity of the system

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorised personnel of resources or access to any college computer system.
Users shall not intentionally develop or use programs for the purpose of harassing other users of the facility, breaking into the system, changing other user's passwords, or damaging system components.

Computer users agree to the proprietary rights of software

Computer software protected by copyright is not to be copied from, into, or by using computing facilities.
Other organisations operating computing and network facilities that are reachable via the College Network may have their own policies governing the use of those resources. When accessing remote resources through College facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organisations.
No user is to install software on any computer or have software stored within their network account.

Connectivity

Users will be provided with Internet, web access and email facilities either by wired, wireless (BYOD) etc. In addition, some College computing resources are available through web services.

Access to these facilities is granted subject to compliance with the legal requirements, behavioural standards and responsibilities specified within this Policy.

All users of the College IT facilities must comply with the relevant parts of UK Law

- You must not try to gain unauthorised access to any computer system anywhere. This is commonly known as hacking and constitutes a criminal offence under The Computer Misuse Act 1990. In certain cases, such activities can also be contrary to other legislation, for example, The Terrorism Act 2006.

- You must abide by any JANET Acceptable Use Policy and College Policies, Standards and Codes of Practice relevant to the use of computers, software and networks that are in place at any time, including those specific to faculties/departments as applicable. The JANET Acceptable Use Policy can been found at https://community.jisc.ac.uk/library/acceptable-use-policy

- You must not do anything maliciously, negligently or recklessly which might cause harm of any sort to any computer system anywhere, or to any of the programs or data on any system. In this context the word harm is taken to mean any kind of damage, and any kind of unauthorised access or alteration.

- If you are reasonably requested to do so, you must justify your use of College IT or networking facilities. You must explain (in confidence, if necessary) what you are doing, and how and why you are doing it. You must make any reasonable changes requested by Technical Services staff representative and comply with any reasonable restrictions placed upon you.

- Unless you have proper permission from the appropriate person or organisation, you must not copy software (even as a backup copy) or share it or make it available in any way to anyone else. Failure to comply with this requirement could constitute a criminal offence under The Copyright, Designs and Patents Act 1988 and The Copyright, etc. & Trade Marks (Offences and Enforcement) Act 2002.

- The Data Protection Act 1998 regulates the use and storage of personal information (i.e. any information which identifies a living individual) on computing systems. It is your responsibility to ensure that your information complies with this law. Failure to do so could result in criminal charges being brought against both you and the University.

- This extends the provision of the Obscene Publications Act and Protection of Children Act to cover the storage and transmission of material by electronic means.

Examples of Misuse

Examples of misuse include, but are not limited to, the activities in the following list.

- Using the College Network to gain unauthorised access to any computer systems.
- Knowingly or carelessly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, phishing, social engineering and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data. This also includes programs contained within an account, or under the ownership of an account that are designed or associated with security cracking.
- Deliberately wasting/overloading computing resources. This includes, but is not limited to, printing multiple copies of a document or printing out large documents that may be available on-line, or that might impact significantly on other users printing resources.
- Moving large files across networks during peak usage periods or prime hours such that it degrades resource performance. Prime hours will be considered to be Monday through Friday from 8am to 5pm. Storing large files on the systems which could compromise system integrity or preclude other user's right of access to disk storage. Appropriate staff may remove or compress disk files that are consuming large amounts of disk space, with or without prior notification.

- Masking the identity of an account or machine. This includes, but is not limited to, sending mail anonymously. Using your account for any activity that is commercial in nature, i.e. activities include, but are not limited to, consulting, typing services, and developing software for sale.
- Posting on electronic bulletin boards materials that violate existing laws or the College codes of conduct.
- Displaying, electronically transmitting/receiving or storing sexually explicit, graphically disturbing, or sexually harassing images or text in a public computer facility, or location that can potentially be in view of other individuals.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner. Files owned by individual users are to be considered private property, whether or not they are accessible by other users.
- Use the internet or email to access or share any material that may be considered to relate to terrorism or extremism nor should such material be downloaded or stored on systems owned or controlled by East Durham College.

Enforcement

The Network Administrator/College Technical Services staff will judge an offence as either major or minor. A first minor offence will normally be dealt with by the Director/Manager/Technical Services Co-ordinator after consultation with the owner of the account, if applicable. In all cases the Manager of the area concerned will be notified. Additional offences will be regarded as major offences.

Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the College, and possible legal action. Violations of some of the policies may constitute a criminal offence.

As with all matters of law and ethics, ignorance of the rules does not excuse violations.

Supporting Documents and Records

- Electronic Communications Guidelines
- Equal Opportunities Policy
- Staff Discipline Procedure
- Grievance Procedure
- Public Interest Disclosure Policy
- Dignity at Work Policy

Please feedback to Quality & Standards any constructive suggestions on how any aspect of the procedure may be clarified or improved