LINCOLN COLLEGE

INTERNET, E-MAIL, AND COMPUTER ACCEPTABLE USE POLICY

POLICY IT/PO/1

SPONSOR

IT Manager

EQUALITY AND DIVERSITY STATEMENT

Lincoln College strives to treat all its members and visitors fairly and aims to eliminate unjustifiable discrimination on the grounds of gender, race, nationality, ethnic or national origin, political beliefs or practices, disability, marital status, family circumstances, sexual orientation, spent criminal convictions, age or any other inappropriate grounds.

LINCOLN COLLEGE INTERNET, E-MAIL, AND COMPUTER ACCEPTABLE USE POLICY

CONTENTS

Para	Contents	Page Number
1	Introduction	2
2	Scope	2
3	Responsibility	2
4	Monitoring	3
5	Acceptable Use	4
6	Unacceptable Use	4
7	Disciplinary Procedure	6

LINCOLN COLLEGE

INTERNET, E-MAIL, AND COMPUTER ACCEPTABLE USE POLICY

1 INTRODUCTION

1.1 The college recognises the need for effective policies which play a key part in the protection of staff and students and in ensuring that hardware and software are used in a manner that is appropriate for resources purchased and owned by the college or operated on the college premises and that the purposes to which these resources are employed relate exclusively to the teaching of students and administration of the college.

2 SCOPE

2.1 This agreement describes and defines acceptable use of hardware, software, and all other IT resources including those resources which are provided by the college and either made available or hosted externally.

This agreement also describes and defines use of these resources which is unacceptable.

2.2 This agreement also covers the use of personal hardware and software which is purchased and owned by the individual where that equipment is operated either on college premises or when the individual should be carrying out teaching, learning, administrative, or other duties.

2.3 All students are affected by this policy including, but not restricted to, learner responsive students (based at college), employer responsive students (based at an employer), and all full time and part time students.

2.4 All staff are affected by this policy including, but not restricted to, teaching staff, tutors, supervisors, administrative staff, and managers.

2.5 Individuals are also encouraged to refer to other related policies and procedures such as; Data Protection Policy, Safeguarding Policy, Disciplinary Procedures, Student Disciplinary Procedure, and Information Security Policy.

3 RESPONSIBILITY

3.1 It is the responsibility of the individual to read, understand, and accept the policy. **All users are automatically presented with a copy of the policy when they first access the college computer network**. Users must acknowledge their understanding before continuing. The college permanently retains a record of the individual's acceptance of the policy until the individual is no longer employed by or attends the college. This record indicates that the individual has read and accepted the policy.

3.2 It is the responsibility of the individual to ensure that all use of the Internet, e-Mail, Computer, and all other hardware and software falls within the definition of acceptable use, and does not constitute unacceptable use as defined in this policy.

3.3 It is the responsibility of all individuals to remain vigilant about the use of Internet, e-Mail, and any other hardware and software by other staff and students. If individuals become aware of unacceptable use, it is their responsibility to report it to their tutor (for students) or to their line manager (for staff).

4 MONITORING

4.1 The college reserves the right to monitor the use of all hardware and software.

4.2 This monitoring includes, but is not limited to:

- The permanent recording of all web sites visited and all Internet resources accessed by individuals.
- The searching and retrieval of web site and Internet resource access by individuals for the purposes of sampling and policing the acceptable use of resources.
- The permanent recording, archiving, searching and retrieval of all e-Mail correspondence and attachments.
- The attempted access of web sites and other Internet resources rejected by the web filtering system.
- The recording of and access to all photographs, e-Mails, texts, and other communications made from or received by College owned mobile computers, mobile phones, smart phones, and other mobile devices.
- All outgoing **and incoming** messages and communications made via College owned equipment.
- All outgoing **and incoming** messages and communications made via personal equipment which is connected to the College network.
- Active monitoring and reporting on attempts to access blocked material in relation to terrorism and extremism.

4.3 The purposes of monitoring activity are:

- The protection of all students and staff under the Safeguarding Policy.
- Ensuring that all use of Internet, e-Mail, and other Computer and Communications related resources adheres to this policy.

4.4 If there is any reasonable belief that any of the regulations in this policy are being broken or that criminal activities are being undertaken, the monitoring records will be accessed and used to ascertain if disciplinary of legal proceedings are appropriate (see section 7).

4.5 The college reserves the right to review monitored activity for the purposes of sampling general use to ensure wide spread understanding of and adherence to the policy.

4.6 In addition to monitoring activity, the college reserves the right to access staff emails during periods of absence (for example during sickness, special leave, maternity leave etc.) to enable work that arrives via email to be carried out by other members of staff.

5 ACCEPTABLE USE

5.1 Any student or member of staff of Lincoln College may use the college's internet access, e-mail, computers, printers, and other hardware and software to support teaching, learning, and research providing it is within the direct scope of the college's activities.

5.2 Any member of staff of Lincoln College may use the college's internet access, e-mail, computers, printers, and other hardware and software to support the administration and operation of Lincoln College.

5.3 All users must correctly identify themselves at all times. Individuals may be asked to show their College ID/NUS Card or Staff ID in any area.

All users will be required to supply their personal user name and password before accessing any computer resources.

Individuals must use their own details only and must not divulge their password to anyone else including staff, students or anyone else not associated with the college.

5.4 Where a PC is available and not required for acceptable college use, it is permissible for college employees to access the Internet for personal use during breaks.

6 UNACCEPTABLE USE

6.1 The following are unacceptable uses of e-mail:

- It is not permissible for staff or students to use the college's e-mail facilities for personal use. If personal e-mails are received, that e-mail must be deleted and not responded to using college facilities.
- Only users who have e-mail accounts specifically created for them may user the college's e-mail facilities.
- Sensitive, private, or personal information must never be sent via e-mail unless being transmitted for work-based purposes following the encryption guidelines in the Security and Disaster Recovery Policy.
- If third party e-mail systems (including Web based e-mail facilities) are used then no reference or connection is to be made or inferred to the college.

- The transmission of unsolicited commercial or advertising material.

6.2 The following are unacceptable uses for Internet access:

- Any access[1] to offensive, obscene or indecent images, data or other material.
- Any access to material which is designed or likely to cause upset, annoyance, inconvenience or needless anxiety.
- Any access to material which could be considered menacing, discriminatory, defamatory, harassing, bullying, fraudulent or confidential/private.
- Any access to material which is for 'leisure activity' (for example playing games) unless this is an integral part of the course.
- Any access to material which that infringes the copyright of another person or organization including unlicensed or illegal software.
- Any access to web sites and resources which are blocked by the college web filtering system by any method.
- Any attempts to access material that is associated with terrorism or extremism.

6.3 The following are unacceptable uses of all IT resources:

- Wasting staff effort or network resources.
- The deliberate corruption or destruction of any hardware, software, files, or data.
- Violating the privacy of others including stealing or plagiarising
- Disrupting the work of others .
- Using resources in a way that denies access to other users including hacking, reckless overloading,
- Any use of equipment for personal use or for storage of personal files (with the exception of section 5.3).
- The introduction of computer viruses or other types of malware
- Unauthorized access to systems, web sites, or data either of the college or third parties.
- Any use of resources which contravenes the Data Protection Act.
- Any use of resources which contravenes the Computer Misuse Act.
- Any use of resources which affects the Safeguarding of students as defined in the Safeguarding Policy.
- Any use of resources which amounts to cyber bullying as defined in the Safeguarding Policy.
- The installation or removal of any software, packages, or software applications.

6.4 Where staff or students use their own equipment (including, but not limited to, laptops, iPads, mobile phones, smart phones, and other mobile devices) on college premises the definitions of acceptable and unacceptable use will apply.

[1] "Any access" includes creating, copying, sending, storing, displaying or receiving

Personal equipment (i.e. equipment that is owned by students and staff) may not be connected to the college network with the exception of personal devices connecting to the StuNet facility.

This facility is specifically provided to enable student owned devices to access the Internet. In this case the definition of unacceptable use will apply.

7 DISCIPLINARY PROCEDURE

7.4 Any infringement of these guidelines may result in disciplinary action, including dismissal, being taken, which will be through the existing disciplinary procedures and in certain circumstances could result in the Police being contacted.

7.5 In these circumstances, the Student Disciplinary Procedure will be applied to students and the Disciplinary Procedures applied to teaching and administrative staff.