Lancaster & Morecambe the College

STUDENT COMPUTER USE
- Play IT Safe

1. Introduction

Computers are provided and maintained for the benefit of all students.

Students are encouraged to use and enjoy these resources and to ensure that they remain available to all.

Any damage, malicious alteration or inappropriate use of the computer equipment may harm their education and that of other students.

To protect all in its care, the College must insist that all students adhere to its rules for acceptable use of the equipment.

The full version of **Lancaster & Morecambe College's IT Security Policy 'Play IT Safe'** and the associated Codes of Practice should be read by all students and can be found on The Hub and on the Virtual Learning Environment front page:

2. HELP

STUDENTS MUST:

- Set their password so it is A MINIMUM OF EIGHT CHARACTERS in length and consists of a mixture of alpha-numeric (*letters and numbers*) characters. Passwords should not be set to names or words which would be easy for someone to guess.
- Change their password at lease once every academic term and more often if possible.
- Contact Computer Services on extension 265 as soon as a virus is detected by the LMC anti-virus software.

STUDENTS MUST NOT:

- Disclose their passwords to others or use passwords intended for the use of others

3. NETWORK RULES

STUDENTS MUST:

- Be aware of the College **Code of Practice for eSafety.**

- Respect, and not attempt to bypass, security in place on the computer systems. Accessing, copying removing or otherwise altering other people's work, or attempting to alter the settings of computers is not acceptable use of the equipment.

STUDENTS MUST NOT:

- Store, install, or attempt to install, programmes of any type on to a computer.
- Use any utility programs or software that can monitor system activity.
- Damage, disable or otherwise harm the operation of computers, or intentionally waste limited resources.
- Use the network for commercial purposes, e.g. buying or selling goods.
- Use the network to harass, harm offend or insult others.
- Play any computer games.
- Use the network unless they are logged on with their own ID.
- Connect any hardware devices to the College network without staff approval.

4. INTERNET RULES

STUDENTS MUST:

- Access the Internet only for study purposes or for College authorised activities
- Respect the work and ownership rights of people outside the College as well as students and staff. This includes abiding by copyright laws.

STUDENTS MUST NOT:

- Use the Internet to obtain, download, send, print, and display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Engage in chat activities over the Internet. This takes up valuable resources which could be used by other people to benefit their studies.
- Use the Internet in class without their tutor's prior permission.
- Download Audio or Video files without their tutor's permission.

5. E-MAIL RULES

STUDENTS MUST:

- Report to their tutor any unpleasant material or messages. Such reports will be treated confidentially and will help protect students.

STUDENTS MUST NOT:

- Give personal information such as address or telephone number to those who make contact through electronic mail.
- Send bulk mail messages ('junk mail' or 'spam' of any kind).

6. REMOTE ACCESS RULES

STUDENTS MUST:

- Read the Code of Conduct for Remote Access before using the remote access facility

STUDENTS MUST NOT:

- Use any personal laptops (using the College network) except in the designated areas whilst complying with the security recommendations of the College

7. INFORMATION SECURITY

STUDENTS MUST:

- Observe and adhere to the College's Information Security policy and the associated Codes of Practice.
- Get permission from the College's Data Protection Officer before storing personal details on any College computer.
- Read the College's Information Security Policy "Play IT Safe" which can be found on The Hub or is available from Computer Services.
- Be aware that student work (other than emails) will be backed up and archived.
- Be aware that the College is required to monitor and log user activity on all networked computer systems.

8. SANCTIONS

- Breaking of these rules will result in withdrawal of access to Information Computer Technology resources.
- Additional action may be taken by the College in line with existing practice regarding inappropriate behaviour. For serious violations, the College disciplinary procedures will be implemented.
- The College reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.
- Students must report to their tutor any security breaches. Such reports will be treated confidentially.
- Computer Services Staff will lock student user accounts immediately after instructed to do so by a member of staff or if a virus is reported by the virus checking software. The Student's tutor will be contacted and the account will remain locked until the Tutor, having spoken to the student, instructs Computer Services in writing to re-instate the account.

9. MONITORING

The College has software and systems in place to record all Internet usage.

These systems are capable of recording (for each and every user) each World Wide Website visit, each chat, newsgroup or e-mail message and each file transfer in and out of our internal networks.

The College reserves the right to monitor/record usage at any time. No College authorised user of the Internet should have any expectation of privacy as to his or her Internet usage.

To be completed prior to a Policy, Procedure being introduced/renewed.

PART ONE: INITIAL SCREENING

Name of policy/Plan/Procedure being assessed: **Play IT Safe – IT Security Policy** **Is this a new or existing policy/function?** Existing √ New ☐	**Name of manager/group carrying out the assessment:** **Martina Hoare – Computer Services Manager.**
1. In which of the listed areas could the new/amended policy, plan or procedure have an impact? These areas follow the College SES NB: This could be positive as well as negative. (please tick box)	√ Gender √ Race and Ethnicity √ Disability √ Sexual Orientation √ Age √ Religion/belief √ Socio-Economic ☐ Pregnancy/Maternity ☐ Gender Reassignment ☐ None expected ☐ Marriage/Civil Partnership
2. What are the risks of introducing this change to any of the above groups?	Risk of access to inappropriate materials and resources Risk of hacking or computer misuse Risk to data
3. What are the expected benefits of introducing this change to any of the above groups?	Common access to information and resources for all staff and students. Secure IT environment Security of data Management of internet access
4. Are there any areas or issues that could impact on the safety of staff or learners?	e-Safety through internet access Unauthorised access to personal data
5. What evidence do you have for the listed areas.	Legal directives – JISC Legal ICT policy and quality standards Safeguarding policy
6. Is this policy/plan/procedure deemed to have a of High, Medium or Low risk?	High
7. Is there any further action to be taken as a result of completing this screening form? *For example, a need to complete a full Equality Impact Assessment or to set the date of a review.*	**Is a full screening Impact Assessment required?** Yes ☐ No √ If yes, please move to complete Part 2 overleaf **Date of review:**
Signed (completing Officer) Martina Hoare…… **Job Title: Computer Services Manager**	**Date of completion of Impact Assessment:**

This document should be securely stored with the relevant policy/procedure

Screening for Equality Impact Assessment (including Safeguarding)

PART TWO: FULL SCREENING

If deemed necessary following completion of Part One then Part Two needs to be completed for a Policy, Procedure being introduced/renewed.

8. **Who has been approached to explore these issues e.g. staff groups, trade unions, student groups, voluntary groups etc.?** (Please give dates and details of contact).	
9. **How have you gained the views of these experts/groups (e.g. letter, meetings, interviews, forums, workshops, questionnaires or any other method)?**	
10. **Please give details of the views of the experts/groups on the issues involved.**	
11. **Taking into account these views and the available evidence, please outline the risks associated with the changes weighed against the benefits.**	
12. **What changes/modifications will now be made to the policy/function in the light of this Impact Assessment?**	
13. **How will these changes/modifications be communicated to interested parties? (i.e. the groups which were adversely affected and those consulted)**	
14. **Is there any further action to be taken as a result of this screening?** (Please give details).	Yes ☐ No √ **Date of review:**
Signed (completing Officer) …… …… **Job Title:**	**Date of completion of Impact Assessment:** 08.07/11

This document should be securely stored with the paperwork for the policy/procedure