

Policy Title	eSafety Policy for Staff
Issue date	October 2011
Author	Clare Holden
Approved by	Information Management Group
Review Date	July 2012
Page	1 of 7

Context and/or Aims

The College Staff eSafety Policy complies with the following policies and legislation:

- [JANET Acceptable Use \(Version 11.0, May 2011\)](#)
- [Defamation Act 1966](#)
- [Criminal Justice and Public Order Act \(1994\)](#)
- [Disability Discrimination Act \(1995\)](#)
- [The Data Protection Act 1998](#)
- [The Copyright Designs and Patents Act \(1988\)](#)
- [The Computer Misuse Act \(1990\)](#)
- [The Freedom of Information Act \(2000\)](#)

Policy Statement

Staff are entitled to have access to the Internet and email both at the main college site, and at outreach centres for research and education purposes, and Loughborough College welcomes this as a means for improving the IT skills of users.

In order to gain a user name and password, staff should complete a registration form which is available in the Personnel Office, and sign to agree to abide by this policy. This process should be signed by the appropriate Team Leader or Manager as part of the New Starter process.

Loughborough College policy on passwords is that they should be 10 characters or more, and should also include at least one number and a character such as a dot. To ensure security they should not include the name or part of the name of the user. Users who wrongly input their passwords five times and fail to log in will be locked out of the system for a period of time, to avoid security breaches. Users should also ensure that they log off correctly to avoid other users gaining access to their desktop and private data.

It should be understood that the College Internet and email service is primarily for work-related purposes, and any use of the system for private use should be outside of normal working hours. Excessive private use of the Internet and email during normal working hours may lead to disciplinary action. Users must accept full responsibility for personal bank data, for example in using the College network when making private purchases online.

Policy Title	eSafety Policy for Staff
Issue date	October 2011
Author	Clare Holden
Approved by	Information Management Group
Review Date	July 2012
Page	2 of 7

The College internet service must not be used for the purposes of private commercial activity by any member of staff.

Internet

There are rules and guidelines that must be followed when using the Internet to ensure that the college complies with current legislation. Loughborough College Management reserves the right to withdraw certain Internet sites, and services, for any reason, and may from time to time gain access to an individual user's search history. History files may be used as evidence in disciplinary or legal proceedings.

The College Internet service is accessed via a proxy server which monitors sites and restricts those which may be in breach of the following rules. Any person found to be deliberately re-routing access to avoid these restrictions will be subject to college disciplinary proceedings. Accessing inappropriate sites may lead to disciplinary action, and in some circumstances may be treated by the College as gross misconduct.

The College takes reasonable steps to protect users from accidental exposure to explicit material. Please report any incidents to itsupport@loucoll.ac.uk

Internet Usage Rules

1. Users must not attempt to access, or upload onto the web, information that is obscene, sexually explicit, racist, defamatory, incites or depicts violence, or describes techniques for criminal or terrorist acts.
2. Users must not intentionally access or transmit computer viruses, or attempt to 'hack' into data that may damage the college network.
3. Users must not infringe copyright - this includes unauthorised copying of images from the Internet without permission, and downloading of music files and commercial screensavers.
4. Staff must not use the College Internet service for private commercial activity.
5. Users must not knowingly undertake any action that will bring the college into disrepute.
6. Users must not attempt to deliberately re-route their connection to avoid the College proxy server, or falsify usage logs in order to escape detection.

Policy Title	eSafety Policy for Staff
Issue date	October 2011
Author	Clare Holden
Approved by	Information Management Group
Review Date	July 2012
Page	3 of 7

Social Networking and Personal Publishing Rules

1. The Executive may take the decision to block some social networking sites for both students and staff in college, and staff who wish to have access should make a special case to the Student and Support Services Manager.
2. Staff are employed by the College to develop and maintain professional relationships with students and to respect the boundaries that come with this responsibility. Staff must not invite or accept students, past or present, to be friends on their personal Facebook, or other social networking sites, and to be aware of the dangers of divulging personal or inappropriate information to students using this medium.
3. When publishing blogs, posts or twitter, staff should remember the following: be professional in all content as they are ambassadors of the College, be responsible and honest in all comments – remember that anything published in an open forum can be picked by the media, and may be available via search engines for many years.
4. Staff should be aware that the information published on social networking sites should not bring the college, any member of staff, or student into disrepute. This includes the publishing of personal opinions or criticism.
5. Staff are advised never to give out personal details of any kind which may identify them, or their location.

Outlook Email and Calendars

Email access opens up the College to additional risks and liabilities, so it is essential that all staff are familiar with this policy and the potential liabilities in using email.

The College email system is monitored and protected by a spam filtering system that is designed to protect staff from spam and other inappropriate email. Staff must be aware that Management reserves the right to gain access to any email document sent by staff to recipients either inside or outside the College, and email sent into the college system from external contacts as part of a disciplinary investigation. Staff should be aware that emails can be recovered, even after deletion, and used as evidence in disciplinary or legal proceedings.

All email references to third parties have the same legal status as they would in any other published form.

Policy Title	eSafety Policy for Staff
Issue date	October 2011
Author	Clare Holden
Approved by	Information Management Group
Review Date	July 2012
Page	4 of 7

Staff email accounts are set at defined limits by the IT Support Team, which will not normally be extended except under special circumstances. Staff need to ensure that their emails are archived or deleted on a regular basis in order to keep mail accounts under the required limits.

Staff outlook calendars are open for review purposes only to all other staff as a default setting. Users should therefore ensure that any confidential appointments have the appropriate privacy settings marked.

This Policy will be reviewed on a regular basis, and revisions may be made as appropriate.

Email Usage Rules

1. Downloading and passing on copyright information, or material, which may be considered to be obscene, abusive, racist or defamatory, will be treated by the college as gross misconduct. Be aware that such material may be contained in jokes or cartoons sent by email.
2. Users must not knowingly send or receive information that will bring the College into disrepute.
3. Staff must never use personal email addresses to communicate with students and should encourage students to use their college email addresses for communicating on college matters.
4. Users must not knowingly send information to sources outside the College, if this might compromise the College's commercial activities.
5. Users must not use the College email system for any private commercial activity. This is strictly forbidden by the JANET acceptable use policy.
6. Information sent by email may become subject to the Data Protection Act, and this must be complied with where appropriate. This also applies to information that may be accessible in other user's calendars.
7. Email must not be used for unsolicited advertising, or sending unnecessary 'jokes' and other non-work information to staff.
8. Persons sending email must not flood the network by sending unnecessary information to all users. This uses bandwidth on the network, and server space, and may prevent important information getting through.
9. Staff should avoid sending documents to large groups of users by email, as this also uses large amounts of bandwidth on the network. Documents should either be placed on the Staff Intranet (SharePoint) or on a shared joint drive, and a link to the document can be sent by email.

Policy Title	eSafety Policy for Staff
Issue date	October 2011
Author	Clare Holden
Approved by	Information Management Group
Review Date	July 2012
Page	5 of 7

Valid Uses of Computers and Network

College Staff are permitted to use College computers and network for the following purposes:

- Preparing coursework assignments and learning materials for their College teaching
- Administrative work in connection with employment and research at college
- Work to increase their knowledge and understanding of computing or software packages, providing this does not contravene any other part of this policy.
- Any other work approved by a member of the Management Group who is responsible for line management of that person.
- Access to the Internet is available on all networked computers throughout the College. Please see the separate policy for Internet use.
- Staff should not use the network for the storage of photographs, videos, games and other multimedia items as these take up large amounts of room on the servers. College videos and photographs should be stored on the college Media Bank which is designed for the purpose. Please contact the eResources Team for help with this.

Equipment

No item of equipment or software should be moved or interfered with in any way by a member of staff, unless specifically instructed to do so by a member of the Computer Services Team. This includes:

- Moving a computer
- Moving a printer, or its lead
- Connecting or disconnecting items of equipment
- Altering settings – such as options for Internet and, printer settings.
- Removing or installing software

Shared computers should be logged-off correctly at the end of each session – using the ‘restart the computer’ choice on the log-off screen.

Computers should be logged off and switched off at the end of each day using the ‘shut down’ option, and the power button. Computer monitors should also be switched off using the power button.

Policy Title	eSafety Policy for Staff
Issue date	October 2011
Author	Clare Holden
Approved by	Information Management Group
Review Date	July 2012
Page	6 of 7

Any machine faults should be reported at once to IT Support preferably by email - itsupport@loucoll.ac.uk

Software

- No software should be installed on or removed from a computer except by prior arrangement with the Computer Services Team.
- Staff are not permitted to make copies of College software; it is an offence under the Copyright, Design and Patents Act (1988) to make unlicensed copies of software

Security

- Users are responsible for their areas and their contents; users must not allow anyone else to use their area or divulge their passwords or other logging in systems to other people – this is a college disciplinary offence for both parties involved.
- Users are responsible for remembering and maintaining their passwords – staff are responsible for the data on their personal drive, - P: Drive, and ensuring that it does not contravene any of the Acts of Parliament listed above.
- Staff should be aware of the risks in leaving computer screens switched on with sensitive data on view in public areas.
- Data on the **J: Drive** will be organised in Team areas – with each Team leader being responsible for data held on the area.

Breach of these rules is a serious disciplinary offence, and may result in the college taking legal action against the offender.

Potential impact on Equal Opportunities

An Equality Initial Screening/Impact Assessment has been conducted and the necessary amendments made to this policy.

Risk Assessments for Computer users can be undertaken by the Health and Safety Officer, and any recommendations from the report will be actioned by the Computer Services Team

Related Documents

- Data Protection Policy
- Data Protection Guide

Policy Title	eSafety Policy for Staff
Issue date	October 2011
Author	Clare Holden
Approved by	Information Management Group
Review Date	July 2012
Page	7 of 7

- College Monitoring Policy