IT and Computer Security Policy

October 2014

Contents

1. Scope

This policy applies to everyone and is non-contractual and without prejudice to your statutory rights.

Loughborough College commits to preserving the confidentiality, integrity and availability of all the physical and electronic information assets. All college information is a valuable asset and must be protected together with the systems, equipment and processes that supports its use.

2. Responsibility

The IT Services Department is responsible for updating this policy.

Everyone is responsible for operating within and maintaining these guidelines.

This policy will be reviewed and updated where applicable on an annual basis unless significant changes are required at any time during the year.

3. Access and Ownership of Information

a) Students are expected to become familiar with and abide by the college IT policies:

- Information Security Policy
- Access Control Policy
- Physical Security Policy
- Anti-Malware Policy
- Network Security Policy
- Cloud Computing Policy

Standards and guidelines for appropriate and acceptable usage of the networks and systems. Everyone will have access to expectations, knowledge, and skills related to information security.

b) It is the responsibility of everyone to protect any college related information that they have created or to which they have been granted access. Such information remains the property of, and confidential to Loughborough College.

c) The college will provide all Students and other users with the information they need in order to carry out their responsibilities in as effective and efficient manner as possible.

d) A policy is in place to automatically lock all computers/devices after 10 minutes of inactivity or if the student is away from the computer/device. The students password must then be entered to regain access to the computer/device.

e) Passwords must not be disclosed or shared with anyone and if asked for must be declined and reported to the IT Department

f) The IT department will remove access/email accounts as requested from the curriculum manager or when a student leaves the college.

g) Specific breaches of confidence, whether within the college or outside, will be regarded as gross misconduct and will be dealt with in compliance with college's student disciplinary procedure, the consequence of which could result in summary expulsion.

h) Loughborough college student emails may be configured on personal mobile phones. Guides are and will be provided from SharePoint on how to configure the device. All measure must be ensured to enforce the General Data Protection Regulation (GDPR) in order to safeguard data and personal information.

4. Security

4.1 Equipment

a) All reasonable steps must be taken to prevent loss, damage and theft of any Loughborough college computer related equipment.

b) Everyone is to take full responsibility for the equipment being used. Laptops should always be returned and must not be left unattended.

c) Computer equipment is the property of the college and should not therefore, be defaced in any way.

d) Any theft or damage must be reported immediately to your tutor and the IT Services Department.

e) All loan equipment must be returned to the college as requested by the IT Department.

f) Moving or relocating of any IT equipment should only be conducted by a member of the IT department. If IT equipment needs to be moved or relocated, you must first contact the IT department.

4.2 Use of Unauthorised Software and Secure Data Storage

a) Software, including fonts is purchased by the college in accordance with software licensing regulations and specific terms of purchase. Under Copyright Law, it is illegal to copy software and can lead to serious penalties which may include fines and/or imprisonment.

b) Software is only authorised if it is licensed and purchased by the college.

c) No unauthorised software may be used or installed on any computer belonging to the college.

d) No copying of software programs is permitted. It is illegal to copy licensed computer software.

e) Documents should be stored on the college networked file servers or Office 365 One Drive where it is both secure and recoverable if required.

f) Making, acquiring or using unauthorised software will be regarded as serious misconduct which will be dealt with in compliance with the college's student disciplinary procedure, the consequence of which could result in summary dismissal.

g) Storage of personal data such as photos, videos and documents is prohibited on the college network. If such documents are found, they will be removed from the system without warning and permanently deleted.

4. Passwords

a) Everyone is expected to become familiar with and adhere by the Access Control Policy to ensure limit breaches of security and potential loss of personal and professional privacy.

5. Computer Virus Protection

Computer viruses are a major threat to the college systems. It is, therefore, vital that all computer users adhere closely to the anti-virus measures set out below;

a) All users are responsible for ensuring that they do not knowingly introduce or transmit computer viruses into the college computer network.

b) Any electronic storage media received from a non-company machine should be virus checked either by the IT Department or a computer approved by the IT Department for the purpose of opening foreign electronic storage.

c) All software must be tested by the IT Department before it is installed. It is not permitted to bring any personally owned storage media or software into the Company unless prior authorisation has been given by the IT Department. This includes sample USBs and CD's, evaluation software and software which may have been obtained through approved supply processes, vendor bulletin boards, academic networks, the Internet and any other public sources.

d) Only equipment approved by the IT Department may be connected to the network or to any individual item of computer equipment. Eduroam is separate from the College network and allows access to internet and Office 365 only.

e) If you discover or suspect that your computer has been infected by a virus, you should take the following steps;

- Note the symptoms and any messages appearing on the screen
- Report the incident to the IT Department
- Stop using the equipment
- Ensure that any disks that are in use are not transferred to any other computers.
- Do not under any circumstances try to remove the virus yourself. This procedure MUST be carried out by experienced IT staff.

f) You must never continue to use or allow anyone else to use any system suspected of having a virus. Misuse of computer equipment relating to virus protection may be regarded as serious misconduct that may result in disciplinary action being taken. .

6. Use of Internet, Company Intranet and Email

a) The Internet is available within the college solely to facilitate learning-related communications and transactions and as a resource to support the objectives of the learner journey.

b) The use of these systems must be in a manner that is consistent with the college's standards of conduct. As a communication tool, using e-mail has the same status in law as communication in writing.

c) All students, and in particular, authorised users of the Internet, email do not breach any of the college policies when sending e-mail, accessing the intranet or Internet.

d) Access to the Internet and email is provided at the discretion of the IT Services Department. Only users who have been given authorisation may use the Internet and e-mail.

e) These services are provided for the purpose of furthering the learner journey. Use of the internet, email and intranet for personal, private or non-business purposes is strictly prohibited. This includes, but is not limited to, advertising, sales of goods, social arrangements etc.

f) Under no circumstances should users display or distribute material which may be deemed discriminatory on the grounds of gender, age, social class, race, ethnic origin, religious belief, disability or moral beliefs.

g) Students must not use the college's intranet, email or internet in a manner that may be deemed defamatory.

h) Students are forbidden from using email, intranet and the Internet to engage in illegal activities or any activities that might harm the college or its reputation in any way. This includes, but is not limited to, accessing sites or distributing emails containing adult material, sites encouraging the use of viruses and computer hacking, sending discriminatory, defamatory, racial or other threatening material and gambling.

i) Messages and Internet sites visited by employees can and will be regularly monitored by the IT Department. Email messages remain the property of the college while on college machines and must be treated with the same confidentiality as any other material stored on the college's systems.

j) All SSL secure internet traffic can and may be read by the college IT support team and inspected to prevent misuse, virus and malware outbreaks.

k) All email activity is monitored to ensure the integrity of the college's intellectual property.

l) Confidential messages should not be sent if the consequences of unauthorised access could be detrimental.

m) Any material that is subject to copyright regulations should not be downloaded, copied or distributed without authorisation and payment if appropriate.

n) Students may only download information or files from the internet if the activity is absolutely necessary for learning purposes.

o) The downloading, distribution and creation of executable files, including screen savers or documents containing “startup” programmes is not permitted without the express permission of the IT Department.

p) Non text files or messages must not be imported on to a college computer unless they have been checked for viruses.

q) If any users are unsure of what constitutes acceptable use of computer equipment and systems, they should discuss their intended use with their tutor or the IT Department in the first instance.

7. Monitoring of Internet and Email Usage

a) The college maintains the right to monitor Internet usage and email usage at any time for the reasons specified in (6) above.

b) A log will be kept of all web sites visited at any time and can be inspected, if required, by the IT Department under authorisation from the Safeguarding Department.

c) Misuse of the college’s Internet and email facility may be regarded as serious misconduct that may result in disciplinary action being taken.

8. Backup Functionality and Audits

a) All students are responsible for ensuring that their college data is backed-up and secure at all times. This can be achieved by using an approved college backup devices or shared drives.

b) The IT Department are responsible for ensuring the file repositories are successfully maintained and backed-up daily.

10. Reporting IT Security Incidents

a) An IT security incident is an event or situation that has or may compromise the confidentiality, integrity or availability of any college’s information. These incidents may include but are not limited to, the loss or theft of any computer or telecommunications equipment, casual browsing by unauthorised users, intrusion of a ‘hacker’ onto the network etc.

b) Everyone must report promptly any actual or suspected incident to their tutor who will then inform the IT Department. The IT Department will advise the appropriate action to resolve and prevent the incident reoccurring.

11. Use of Cloud Technologies

a) The use of cloud technologies such as Dropbox and OneDrive must be registered with a college email address and not a personal email address if the account is to be used for college Data.

12. Passwords

Passwords are an important aspect of computer security. A poor password may result in breaches of security and potential loss of personal privacy. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.
As such, are responsible for taking the appropriate steps, select and secure their passwords.

12.1 General Guidance for Passwords

a) Passwords are used for various purposes. Some of the more common uses include: user level accounts, web applications, email accounts. Everyone should be aware of how to select strong passwords.

b) The College has a principle password complexity of 11 characters or more and must including letters, numbers and symbols.

c) Passwords must not be disclosed or shared to anyone. If you have shared your password or concerned that someone knows it, please contact the IT department

d) Passwords should never be written down or stored on-line.

e) Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

f) Guidelines for strong and weak passwords can be found in the Access Control Policy.

12.2 Computer Passwords

a) It is the responsibility of student to protect any company related information that they have created or to which they have been granted access. Such information remains the property of, and confidential to the company in compliance with the declaration of confidential information agreement.

c) If sensitive information is held on a PC, while you carryout activities away from the PC please ensure you lock the computer until you require use to prevent unauthorised access.

12.3 Data Protection

We recognise the importance of respecting the personal privacy of all of our employees, learners, employers and colleges and any other respective stakeholders to whom we deal with as well as the need to build in appropriate safeguards during the collection, storage, processing and utilisation of personal data in accordance with the GDPR.

We this in mind we are registered with the Information Commissioner's Office (ICO). This is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

We are entitled to hold personal data held for 5 main purposes:

1. Staff Administration
2. Advertising, Marketing & Public Relations
3. Accounts & Records
4. Education
5. Consultancy and Advisory Services

Within these 5 key areas the register outlines the purpose description, the data subjects, data classes, recipients and transfers.