IT ACCEPTABLE USAGE POLICY

CITY OF LONDON COLLEGE
A University Sector Premier College

Contents

1. Introduction

This Acceptable Usage Policy covers the security and use of all City of London College's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. It applies to all resources provided for City of London College Students, Staff and consultants/contractors, including but not limited to:

- Audio-visual equipment
- Blogs
- Computers
- Computing software
- E-mail
- Fax
- Instant Messaging and Collaborative applications such as Microsoft Lync
- Internet and Intranet
- Mobile devices including laptops, mobile phones, smart phones, PDA's, tablets, etc
- Network
- Photocopiers
- Printers
- Remote access service e.g. XA (Xternal Access)
- Scanners
- Telephone or videophone
- Text
- Voicemail
- Portable memory/storage devices
- BYOD (bring your own device) used for University business.

This policy applies to all City of London College's employees, students, contractors and agents (hereafter referred to as 'individuals').

This policy applies to College business conducted on site and off site at other premises and most specifically at home or place of residence. It applies to equipment supplied by the College and equipment supplied by the employee or student.

This policy applies to all information, in whatever form, relating to City of London College's business activities worldwide, and to all information handled by City of London College relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by City of London College or on its behalf.

The College believes it is important that staff have a clear understanding of the expectations that the College places on them and the standards to which they are expected to work. These relate both to the work they undertake and the way in which they conduct themselves at work.

This policy introduces some key implications on all staff and students to ensure compliant use of College systems and infrastructure.

1. Any device used to connect to the College network must be via an authenticated user id and password issued by the College and any personal device will have a local secure PIN or password activated on the physical device before connection.
2. Personal data remains the responsibility of the College data controller irrespective of where it's stored or located. This includes where it's stored on a personally owned device or where it's located via cloud based storage facilities.
3. Personal data regarding College data subjects (staff and students) must not be stored or downloaded to personally owned devices or cloud based storage facilities such as drop box, google docs or one drive or equivalent.
4. Data protection laws have personal implications on individual employees and students who do not follow policy or the law in relation to personal data subjects compliance. Failure to comply with this policy may lead to disciplinary action and ultimately dismissal or separate legal action.
5. Memory sticks provided by the College or provided by the employee/student must not be used for personal data transfer or storage. Any information should be password protected on these devices.

2. Computer Access Control – Individual's Responsibility

Access to the City of London College IT systems is controlled by the use of User IDs, and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the City of London College's IT systems.

Individuals must not:

- allow anyone else to use their user ID/token and password on any City of London College IT system;
- leave their user accounts logged in at an unattended and unlocked computer;
- use someone else's user ID and password to access City of London College's IT systems;
- leave their password unprotected (for example writing it down);
- perform any unauthorised changes to City of London College's IT systems or information;
- attempt to access data that they are not authorised to use or access;
- exceed the limits of their authorisation or specific business need to interrogate the system or data;
- Connect any non-City of London College authorised device to the City of London College network or IT systems;
- store City of London College data on any non-authorised City of London College equipment;
- give or transfer City of London College data or software to any person or organisation outside City of London College without the authority of City of London College.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

3. Internet and email Conditions of Use

Use of City of London College internet and email is intended for business and educational use. Personal use is permitted where such use does not affect the individual's business or academic performance, is not detrimental to City of London College in any way, not in breach of any term and condition of employment and does not place the individual or City of London College in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- use the internet or email for the purposes of harassment or abuse;
- use profanity, obscenities, or derogatory remarks in communications;
- access, download, send or receive any data (including images), which City of London College considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material;
- use the internet or email to make personal gains or conduct a personal business;
- use the internet or email to gamble;
- use the email system in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam;
- place any information on the Internet that relates to City of London College, alter any information about it, or express any opinion about City of London College, unless they are specifically authorised to do this;
- send unprotected sensitive or confidential information externally;
- forward City of London College mail to personal (non-City of London College) email accounts (for example a personal Hotmail account), unless specifically authorised to do so;
- make official commitments through the internet or email on behalf of City of London College unless authorised to do so;
- download copyrighted material such as music media files, film and video files, without appropriate approval;
- in any way infringe any copyright, database rights, trademarks or other intellectual property;
- download any software from the internet without prior approval of the IT Department;
- connect City of London College devices to the internet using non-standard connections.

4. Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, City of London College enforces a clear desk and screen policy as follows:

- personal or confidential business information must be protected using security features provided for example secure print on printers;
- computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended;
- care must be taken to not leave confidential material on printers or photocopiers;

- all business-related printed matter must be disposed of using confidential waste bins or shredders.

5. Working Off-campus

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- working away from the campus must be in line with City of London College remote working policy;
- equipment and media taken off-campus must not be left unattended in public places and not left in sight in a car;
- laptops must be carried as hand luggage when travelling;
- information should be protected against loss or compromise when working remotely (for
- example at home or in public places);
- laptop encryption must be used;
- particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets, they must be protected at least by a password or a PIN and, where available, encryption.

6. Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring confidential data. Only City of London College authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

7. Software

Individuals must use only software that is authorised by City of London College on City of London College's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on City of London College computers must be approved and installed by the City of London College IT department.

Individuals must not store personal files such as music, video, photographs or games on City of London College IT equipment.

The IT department has implemented centralised, automated virus detection and virus software updates within the City of London College. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- remove or disable anti-virus software;
- attempt to remove virus-infected files or clean up an infection, other than by the use of approved City of London College anti-virus software and procedures.

8. Telephony (Voice) Equipment Conditions of Use

Use of City of London College voice equipment is intended for business use. Individuals must not use City of London College's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- use City of London College's voice for conducting private business;
- make hoax or threatening calls to internal or external destinations;
- accept reverse charge calls from domestic or International operators, unless it is for business use.

9. Actions upon Termination of Contract

All City of London College equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to City of London College at termination of contract.

All City of London College data or intellectual property developed or gained during the period of employment remains the property of City of London College and must not be retained beyond termination or reused for any other purpose.

10. Monitoring and Filtering

All data that is created and stored on City of London College computers is the property of City of London College and there is no official provision for individual data privacy, however wherever possible City of London College will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. City of London College has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990;
- Data Protection Act 2018;
- Counter Terrorism and Security Act 2015;
- Prevent Duty Guidance 2015.

It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department or the IT helpdesk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with City of London College disciplinary procedures.

11. Policy Review

This policy will be reviewed on an annual basis, or if there is a change in legal or other business or academic related requirement.

Review date	*Description*	*Reviewer*
30/11/2022	IT Acceptable Usage Policy	Academic Director

Document history:

Version date	*Description*	*Author*
24/11/2016	Policy approved and accepted by Academic Board	Task and Completion Committee
30/11/2017	IT Acceptable Usage Policy	Academic Director
30/11/2018	IT Acceptable Usage Policy	Academic Director
30/11/2019	IT Acceptable Usage Policy	Academic Director
30/11/2020	IT Acceptable Usage Policy	Academic Director
30/11/2021	IT Acceptable Usage Policy	Academic Director