ICT and Digital Acceptable Use Policy

Revised December 2022

ICT and Digital Acceptable Use Policy

1 Introduction

City Lit seeks to promote and enable the positive and extensive use of Information and Communications Technology (**ICT**) in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires defining appropriate and legal use of the technologies and services made available to employees, students and other authorised users. (**Users**)

In accessing City Lit's ICT network or services, or using personal devices to carry out work on behalf of City Lit all users will be deemed to have accepted the terms of this policy. This policy may be updated from time to time, in order to comply with legal and College requirements.

2 Purpose

This policy is intended to provide a framework for the use of the College's network or services. It should be interpreted such that it has the widest application so as to include new and developing technologies and uses, which may not be explicitly referred to.

The use of City Lit's networks and information systems is subject to the JANET Acceptable Use policy.[1]

3 Scope

This policy applies to all users of the City Lit network. The City Lit network comprises all computing, telecommunication, and networking facilities provided by the College, and extends to all computing devices, either personal or College owned, connected to systems and services supplied.

This policy applies to all employees of the College, individuals studying at the college or using the facilities such as the Learning Centre. Employees are defined as all persons working at the College or on our behalf in any capacity, including employees at all levels, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with the College, wherever located.

4 Unacceptable activities

The following is a list of activities that are unacceptable for any user at any time when accessing City Lit's ICT network or services, or using personal devices to carry out work on behalf of City Lit. This list is not exhaustive:

[1] https://community.jisc.ac.uk/library/acceptable-use-policy

- Any activities which would be incompatible with our values.
- Downloading, manipulating, storing, creating, transmitting and / or viewing material that could be considered:
    - indecent
    - obscene
    - hateful
    - violent
    - extremist[2]
    - threatening
    - abusive
    - defamatory
    - harassment, bullying and/or victimisation
    - as causing unwanted damage or distress.
- Unauthorised use of another user's logon credentials.
- Profit or gain-making activities not sanctioned by City Lit.
- Private or personal interests or business, where such use is deemed to be excessive or unreasonable, especially in the use of Internet, Social Media or electronic mail services.

The network must not be deliberately used for activities having, or likely to have, any of the following characteristics:

- Deliberately or recklessly compromising the security of our IT systems and network.
- Seeking to gain unauthorised access to data.
- Disrupting the work of other users or the correct functioning of the network.
- Denying access to the network and its services to other users.
- Wasting resources (e.g. people, capacity, computer, consumables).
- Compromising the privacy of users or confidentiality of data.
- Propagating unsolicited commercial or advertising material, chain or junk emails.
- Political activities including campaigns, petitions or fund raising relating to party political and single issue political campaigns or events without authorisation.
- Personal use or customisation of IT equipment situated in public areas.
- Infringing copyright or licensing agreements.
- Creating or transmitting material with the intention to defraud.
- Introducing computer viruses, Trojans or other malicious software.
- Downloading, installing or removing software without authority.
- Deliberately or recklessly corrupting or destroying another user's data.
- Playing computer games.
- Any illegal activities.

[2] As defined by the Preventing radicalisation policy

Users shall not:

- introduce data-interception, password-detecting or similar software or devices to the network.
- seek to gain unauthorised access to restricted areas of the network.
- access or try to access data where the user knows or ought to know that they should have no access.
- carry out any hacking activities; or
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

5 Online Learning Netiquette

Students are asked to observe the college's online learning netiquette. 'Netiquette' (short for 'net etiquette') refers to the rules of good online behaviour which are intended to facilitate a positive, constructive remote learning environment. Full guidance is available on the City Lit website help centre.

6 Internet

This section covers acceptable use when accessing the internet, personal websites, blogs, and other related activities.

If you consider that you need to undertake any activity that may be misunderstood or considered an unacceptable activity you should:

- reconsider whether your research is appropriate.
- agree your activity with your manager or tutor before undertaking the activity[3].

Employees may use the internet for reasonable personal use, this must be undertaken in a user's own time, normally before/after work or whilst on a break. Any such use must not interfere with individual work responsibilities or affect the quality of service.

If unsure, employees must consult the Digital Learning team before copying material from the internet as it may be subject to copyright.

City Lit reserves the right to apply filters to limit access to websites that contain inappropriate, offensive or illegal content e.g. obscene or pornographic, sexist, racist, terrorist, discriminatory or other offensive material.

7 Social Media

This section covers the use of social media both in a professional and personal capacity when discussing the College.

If employees identify themselves or are identifiable as employees of City Lit online then they are representing City Lit, with the potential to reflect on the City Lit brand and reputation. It

[3] Note: There are certain activities that will always remain unacceptable, e.g. if against the law.

is expected that you would support City Lit in a professional manner and be respectful to City Lit, other employees, students, partners and competitors.

Do not reference our partners, students or business customers without their express consent. The City Lit logo may not be used without consent on personal blogs, social networking sites and personal websites.

Where there is a link to City Lit, personal blogs, social media postings, websites etc. they must have clear disclaimers that the view expressed by the author is that of the author alone and does not necessarily represent the views of City Lit. Any information appearing in a personal posting must comply with our confidentiality and disclosure policies.

Social Media must not be used by employees to promote City Lit financial discounts without authorisation from the Director of Marketing, PR & Communications.

8 Email, Teams and other messaging services

The section covers the use of communication and collaboration services such as Email, Teams and other messaging services. Employees are expected to communicate in a professional manner.

Emails must be managed as a business document and filed in an appropriate filing system to aid retrieval. Emails must be deleted in accordance with the City Lit records retention schedule.

External email messages will automatically receive a confidentiality footer prior to dispatch.

All external email messages originating or received on our computer systems are the property of City Lit and will be automatically scanned.

Emails, Teams and other messaging services must be considered open documents/ communications and disclosable to a wide audience. All writers must think carefully about what is said about other persons or organisations when composing messages. Users must only write that which they would speak in an open forum and must be aware that UK legislation including the laws of libel applies to electronic documents as well as manuscript. Users must not copy, download or forward material that is libellous or otherwise unlawful.

Communications must be disclosed if a request is received to view them e.g. a personal data subject access request. Once a request has been received communications must not be deleted or removed to obstruct the request.

Users must not send discriminatory, biased or other inappropriate communications, or use aggressive, abusive or deliberately antagonistic language.

Users must be vigilant for spam and malicious emails and be aware of opening attachments, even if they purport to come from a recognised address.

- Suspicious attachments must be verified by IT Services before opening.
- Employees must forward spam emails to spam@citylit.ac.uk for inspection.

Employees must ensure that our standard format is used for both internal and external email signatures and that appropriate out of office messages are displayed.

Marketing emails must only be sent using Dotmailer, the City Lit marketing email platform, unless permission has been obtained from the Director of Marketing, PR & Communications to use an alternative method.

Employees must only use their City Lit email account when emailing each other, external contacts or students. Personal email accounts must not be used to conduct City Lit business or forward documents to a personal address.

9 Cloud Services

Permission to use Cloud Services (Software as a Service), Cloud Storage or Apps that are not currently enabled by the College must be submitted to IT Change Board to ensure a coordinated approach in decision making.

Unauthorised usage of Apps or Storage creates a security risk to the College and will be considered a breach of this policy (see Section 16).

10 Audio Communications

Audio communications tools include telephones (both land line and mobile). Internet (VOIP phones) and audio-conferencing services. Employees are expected to use these communication channels in a courteous and professional manner at all times.

Employee personal use of City Lit's telephone system may be used for occasional short, urgent or emergency calls.

All College issued mobile phones must be password protected and usage should be restricted to the monthly allowances of the tariff.

11 Equipment

Employees are responsible for the maintenance and safekeeping of all ICT equipment in their possession or they have responsibility for. All City Lit equipment must be returned on termination of contract or period of service for redistribution or secure destruction.

Ensure equipment is physically secure against loss, theft or use by unauthorised users. If you are unsure how to do this then speak to IT Services. Ensure that devices are password or PIN protected.

Ensure devices are made available to IT Services for mandatory software upgrades when requested.

Software may only be installed on City Lit equipment if covered by a licence and authorised by IT Services to ensure compliance, to prevent the introduction of viruses, and to prevent the introduction of sub-standard software that might interfere with other applications. Software from City Lit machines may not be transferred to other machines.

12 Use of Personal devices (BYOD/WFH)

Staff can only work remotely via VPN using a City Lit managed device. Staff cannot VPN from their private machines. Staff working abroad need to request access in advance (detailing the business need) for the limited time needed.

13 Security

It is the responsibility of all users to comply with City Lit’s Data Protection Policy regarding the safeguarding of personal information and only use software that is licensed to City Lit.

It is your responsibility to ensure that any equipment assigned to you or in your possession is kept as securely as possible, particularly if used off-site, both to reduce the risk of unauthorised access and to safeguard against loss or damage. Equipment should be password protected. Files stored outside the network on shared devices should be password protected.

If equipment is lost or stolen this must be reported immediately to IT Services. If equipment was stolen whilst in your possession you must obtain a Police crime number and report this to IT services if requested. You must also cooperate with any investigation surrounding the circumstances of the loss of theft.

Software or Apps may only be installed if covered by a licence and authorised by IT Services to ensure compliance, to prevent the introduction of viruses, and to prevent the introduction of sub-standard software that might interfere with other applications. Software or Apps from City Lit machines may not be transferred to other machines without permission.

Users must not circumvent security processes or bypass network access controls that are in place, i.e. must not “hack” into the network or bypass Internet access controls e.g. by using proxy services.

14 Remote/Home and Mobile Working Arrangements

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended where possible that the office area of the house should be kept separate from the rest of the house. Equipment must be secured within a locked room or locked cabinet when not in use.

Users must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computing device.

Users are recommended to avoid keeping removable media devices and paper documentation with or in close proximity to the portable computing device when not in use.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be stored in locked rooms or locked cabinets when not in use.

Paper documents should be collected from printers as soon as they are produced and not left where they can be casually read.

Waste paper containing personal or other business sensitive information must be shredded using a cross cut shredder.

15 Monitoring

Automated scanning of employees, students' and third parties' external email and Internet access is undertaken as a control mechanism to detect abuse or inappropriate language, prevent malicious code from entering the network, stop viruses and to comply with JISC security requirements for the use of the JANET connection. Any monitoring will be carried out in accordance with relevant legislation[i].

People who observe or become aware of other employees or students accessing inappropriate content should report this immediately to an appropriate manager.

The content of specific transactions or files will not be routinely monitored unless there is a suspicion of improper use.

Requests to monitor email accounts or internet usage must be approved by the Executive Director – People or authorised representative. Any monitoring activity must be proportionate to the level of event being investigated.

All email and voicemail messages originated or received on City Lit computer and telephone systems are the property of City Lit. If an individual is absent from work, City Lit may authorise access to their messages for business continuity purposes.

An automatic back up of City Lit Information Systems including email and Internet access will be administered by IT Services and held offsite for the purposes of business continuity.

16 Breaches of this policy

Improper use or abuse of systems, networks or facilities or failure to follow this policy may lead to action under the employee Disciplinary procedure or the Student conduct procedure, which could lead to dismissal and/or reporting to any relevant authority as appropriate.

In the event of a breach of this Acceptable Use Policy by a User the College may at its sole discretion:

- restrict or terminate a User's right to use the College's Network.
- withdraw or remove any material uploaded by that User in contravention of this Policy; or
- where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

Action taken by City Lit does not mean that the individual may not also be liable to civil or criminal action in the courts.

Executive Owner	Chief Financial officer
Policy Owner	Data Protection Officer
Approval Body	Governing Body
Date Approve	5 December 2023
Review Period	Annual
Next Scheduled Review Data	Every year from date approved

Version tracking

Versions	**Date**	**Author**	**Reason for changes**
2.3	27/6/19	Graham Jennings	Updates to definition of staff and use of email (7.11)
3.0	11/2/20	Graham Jennings	Renaming of policy. Significant updating or wording particularly for sections on communications and cloud communications to reflect new developments in IT provision
3.1	13/2/20	Graham Jennings	Minor text changes including changing name to ICT and Digital Acceptable Use Policy
4.0	8/2/21	Graham Jennings	New sections added to incorporate online netiquette and home working
4.1	23/6/21	Graham Jennings	Section 12 updated to align with Information Security Policy
4.2	28/01/22	Graham Jennings	Update of section 12 to comply with Cyber Essentials requirements
4.3	December 2022	Graham Jennings	Updated to reflect new working practices following IT incident.

Classification

Document Status	Active
Document Classification	Open

[i] Data Protection Act 2018, Regulation of Investigatory Powers Act 2000, Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000