Acceptable Use of IT Policy

Table of Contents

Acceptable Use of IT Policy

Collective Acting Studio provides its users with access to state-of-the-art Information and Communication Technology (ICT) equipment and a wide range of electronic resources. All users need to be aware of what constitutes the Acceptable Use of these resources to enable them to be used in a safe and secure manner. This page outlines the policies relating to both ICT and e-resources and facilities.

For all our users; staff, students, visitors and any others, using our technology infrastructure constitutes an undertaking to abide by this acceptable use policy and the legal requirements implicit and explicitly contained within.

For the purposes of this policy, designations include staff and students at collaborative partners. You are reminded that accessing COLLECTIVE ICT systems and resources via the Remote Desktop service you are bound by the laws and regulations in the UK as well as any applicable laws in the country from which you are connecting.

Purpose

The purpose of an Acceptable Use Policy is to ensure the proper use of all the Studio's ICT facilities and resources.

Access to the Studio's ICT facilities and resources requires users to accept certain responsibilities and obligations. All users must be aware of and comply with the JANET Acceptable Use Policy, which covers all UK HE academic and research network activity.

Use of IT and associated resources should always be legal and ethical and reflect academic integrity and the standards of the Studio community.

Authorisation

To use the ICT facilities in the Studio, you must first be authorised. For students, this will require your matriculation number and password, which are distributed at matriculation. Staff will receive a confidential mailing containing notification of their username and password. Your matriculation number/username and password are for the exclusive use of the individual to whom they are allocated. You are responsible and accountable for all activities carried out under your matriculation number/username and password.

2

Privacy and Monitoring

It should be noted that systems staff, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files, stored on a computer which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances, appropriately privileged staff will take all reasonable steps to ensure the privacy of service users.

The Studio fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit, in line with its rights under the Regulation of Investigatory Powers Act 2000. Reasons for such monitoring may include the need to:

- Ensure operational effectiveness of services
- Prevent a breach of the law, this policy, or other Studio policy
- Investigate a suspected breach of the law, this policy, or other Studio policy
- Monitor standards

Access to staff files, including electronic mail files, will not normally be given to another member of staff, unless authorised by the appropriate line manager, Head of Operations, or nominee, who will use their discretion, in consultation with a senior officer of the Studio, if appropriate. In such circumstances, the Senior Leadership Team will be informed and will normally be consulted prior to action being taken. Such access will normally only be granted in the following circumstances:

- Where a breach of the law or a serious breach of this or another Studio policy is suspected
- When a documented and lawful request from a law enforcement agency such as the police or security services has been received
- On request from the relevant Senior Leadership Team, where the managers or co-workers of the individual require access to e-mail messages or files, which are records of a Studio activity and the individual is unable, e.g. through absence, to provide them

The Studio sees student privacy as desirable but not as an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been received, systems staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct academic work-based reason for requiring such access.

After a student or member of staff leaves the Studio, files which are left behind on any computer system owned by the Studio, including servers and including electronic mail files, will be considered to be the property of the Studio. When leaving the Studio, staff should

3

make arrangements to transfer to colleagues any e-mail or other computer-based information held under their account, as this will be closed on their departure.

All monitoring and data access activities will be conducted in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The Studio is committed to protecting user privacy while balancing this with our legal and operational obligations.

Acceptable Use of IT

Studio ICT and electronic resources are provided to facilitate your work as a member of the Studio community, specifically for educational, training, research or administrative purposes. Any other uses are a privilege and not a right and must never take priority over the needs of those who require the facilities for directed academic work.

The Studio does not block or filter keywords or search terms, nor does it prevent you from accessing specific sites. That does not mean, however, that you can access or download pornographic or other offensive or objectionable material.

You should bear the following in mind:

- You must not share your COLLECTIVE username and password with anyone else. This will result in your account being disabled immediately. For students, if your account has been disabled then you must appeal for its reinstatement. This must be done in the first instance to your Dean of School. There is no automatic reinstatement. Staff should contact Assist helpdesk.
- You must never use Studio ICT systems to alarm or inconvenience others.
- You must not display anything on your screen which is likely to cause offence or upset other users. However, it is recognised that sometimes it is necessary to display material which is medical in nature, in relation to some programmes/modules.
- You must respect other people's electronic privacy. In particular, you may not use your COLLECTIVE accounts to distribute spam and other chain emails.
- For your own security, you should be careful who you share your COLLECTIVE email and other contact details with.
- You must never pass off other people's work as your own. The Studio produces a guide to referencing, "Write and Cite" which is available online.
- You should not use data which is confidential or not already in the public domain in your work without first consulting the author; there may be copyright or data protection implications.
- You must not maliciously damage or interfere with any item of hardware.

Anyone found abusing COLLECTIVE ICT systems will usually be cautioned in the first instance. Continued abuse will lead to your account being disabled. This means that you will be unable to access any of the networking and communications services. In cases of serious

4

abuse, your account will be disabled immediately. Serious abuse includes the sharing of your username and password.

Forms of Unacceptable Activities

Unacceptable activities can take a variety of forms. Some examples of behaviour which is unacceptable are listed below:

- Transmitting or downloading obscene or offensive material

- Transmitting or downloading threatening material, or material intended to harass or frighten

- Transmitting or downloading defamatory material

- Infringing copyright (see below)

- Hacking, attempted hacking or other deliberately disruptive activities such as introducing viruses to computer equipment
  Sending a bulk email to everyone in the Studio

- Interfering with hardware or software configurations

- Installing or attempting to install unauthorised software to COLLECTIVE ICT equipment

- Adding software to Studio computer equipment

- The use of COLLECTIVE ICT services and equipment to distribute unsolicited advertising (spam), to run a business or similar activities

- Downloading or distributing pirated software or data;

- Viewing or hosting of any illegal streaming content.

- Any other activities that disrupt COLLECTIVE ICT services

AI USE

Artificial Intelligence (AI) Tools Students and staff may use AI tools for legitimate educational and administrative purposes, subject to the following conditions:

- **Permitted uses**: Research assistance, brainstorming, drafting outlines, language translation, technical troubleshooting, and administrative tasks where explicitly approved by tutors

5

- **Prohibited uses**: Generating assessed work content, creating final submissions, replacing individual learning and creative development, producing work presented as original thought
- **Disclosure requirement**: Any use of AI tools must be declared in submissions with details of the tool used, prompts given, and extent of assistance received
- **Module-specific guidance**: Some modules may have specific AI permissions or restrictions - students must check assessment briefs
- **Creative integrity**: In performance and creative modules, AI may assist with research but must not replace the student's own creative process and artistic development

Failure to declare AI use constitutes academic misconduct and will be treated as contract cheating.

Social Media Use

When using social media, whether for personal or Studio-related purposes, users must:

- Be mindful of the Studio's reputation
- Respect others' privacy and feelings
- Not share confidential information
- Make clear when views expressed are personal rather than representing the Studio
- Adhere to the same standards of behaviour as in other forms of communication
- Not engage in any activity that could bring the Studio into disrepute
- Be aware that social media posts can have long-lasting consequences

Data Protection

All users must comply with data protection laws and Studio policies when handling personal or sensitive data. This includes:

- Only collecting and storing necessary data
- Keeping data secure and confidential
- Only using data for its intended purpose
- Deleting data when no longer needed
- Reporting any data breaches immediately to the designated data protection officer
- Ensuring any personal data transferred outside the EU is done so in compliance with GDPR
- Respecting individuals' rights regarding their personal data, including the right to access, rectify, and erase data

Users should familiarise themselves with the Studio's Data Protection Policy 2018 for more detailed guidance.

Cybersecurity

All users must comply with data protection laws and Studio policies when handling personal or sensitive data. This includes:

- Only collecting and storing necessary data
- Keeping data secure and confidential
- Only using data for its intended purpose
- Deleting data when no longer needed
- Reporting any data breaches immediately to the designated data protection officer
- Ensuring any personal data transferred outside the EU is done so in compliance with GDPR
- Respecting individuals' rights regarding their personal data, including the right to access, rectify, and erase data

Users should familiarise themselves with the Studio's Data Protection Policy 2018 for more detailed guidance.

Prevent Duty

Collective Acting Studio has a statutory obligation under the Counter-Terrorism and Security Act (2015) to have 'due regard to the need to prevent people being drawn into terrorism'. This is known as the Prevent Duty.

In compliance with this duty:

- All users are advised that accessing, creating, or distributing extremist material is strictly prohibited and may result in disciplinary action and/or referral to relevant authorities.
- The Studio monitors and filters internet usage to prevent access to extremist materials.
- Staff are trained to recognise signs of radicalisation and to respond appropriately.
- We provide support channels for students who may be vulnerable to extremist ideologies.
- We promote fundamental British values and encourage open dialogue on controversial issues within appropriate academic contexts.
- We partner with local Prevent coordinators and police to stay informed about risks and best practices.

Users should be aware that their online activities may be monitored as part of our Prevent Duty implementation. Any concerns about potential radicalisation should be reported to the Designated Safeguarding Lead: Joseph Junkere.

It's important to note:

7

- The Terrorism Act (2000) makes it an offence to collect or make a record of information likely to be useful to a person committing or preparing an act of terrorism, or to possess a document or record containing such information.
- The Terrorism Act (2006) makes it an offence to disseminate terrorist publications to encourage others to engage in terrorism.

Use of Copyright Software or Datasets

By accessing COLLECTIVE ICT systems, you also agree to the following with regard to copyright:

That usage of any Software, Computer Readable Dataset or Courseware or other similar material, hereafter referred to as "the Product", issued or otherwise made available is subject to the following conditions:

- You will ensure that all the requirements of the agreements, contracts and licences under which the Product is held by the Institution will be maintained. (Copies of the relevant agreements, contracts and licences may be seen by application to the School or Department which made the Product available)

- You will adhere to the regulations governing the use of any service involved in the provision of access to the product whether these services are controlled by this institution or by some other organisation
You will not remove or alter the Copyright Statement on any copies of the Product used by yourself

- You will ensure the Security and Confidentiality of any copy released to yourself and will not make any further copies from it or knowingly permit others to do so, unless permitted to do so under the relevant licence

- You will use the Product only for purposes defined and only on computer systems covered by the agreement, contract or licence

- You will only incorporate the Product, or part thereof, in any work, program or article produced by yourself, where this is permitted by the licence or by "Fair Dealing"

- You will only incorporate some part or version of the Product in any work produced by yourself with the express permission of the Licensor or unless this is permitted under the Agreement

- You will not reverse engineer or decompile the software products or attempt to do so, unless this is explicitly permitted within the terms of the Agreement for the use of the Product

- You will return or destroy all copies of the Product at the end of the programme/year/period of employment or when requested to do so.

8

Legal Constraints

- You must adhere at all times to appropriate statutory law such as the Computer Misuse Act 1990, Defamation Act 1996 and the General Data Protection Regulations and not commit the common law crimes of theft, reset or fraud.

- You should be aware that the **Terrorism Act (2000) 1/section/1** makes it an offence for an individual to collect or make a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism; or to possess a document or record containing information of that kind (e.g. a terrorist training manual).

- You must undertake to comply with the Copyright Designs and Patents Act 1988 and the provisions of the Studio's licence with the Copyright Licensing Agency and with any other applicable legislation, statutory instrument or regulation

- You should always consider the provisions of the General Data Protection Regulations when storing data on a computer. Please review the Studio's Data Protection Policy 2018.

- You should be aware of the Regulation of Investigatory Powers Act 2000 when making use of ICT systems

- You must respect the intellectual property rights, copyright and moral rights of authors
  You must undertake to abide by all licence agreements for software entered into by the Studio with other parties (see below)

- You may only use software and/or information provided by the Studio for educational purposes as a member of the Studio

Code of Conduct when Using our Facilities

All users at COLLECTIVE shall:

- Accept individual and collective responsibility for maintaining a healthy working, studying and living environment within the Studio, respecting the institution's policies on equal opportunities and anti-harassment and ensuring that their conduct complies with these policies

- Accept individual and collective responsibility for keeping a clean and safe working and studying environment, ensuring personal guests act in an appropriate manner. Anything which you believe constitutes a health and safety hazard must be reported immediately to Reception

9

- Have a mutual respect for others especially with regard to differing cultures

- Have an individual and collective responsibility to contribute to a study environment that promotes scholarship and learning. All persons should be considerate of the needs of others for an appropriate study environment and share a common goal in learning

- Have an individual and collective responsibility to ensure that the safety of themselves and others is not compromised

- Ensure that their use of the computer systems and networks is always legal and ethical and reflects academic integrity and the standards of the Studio community

- Have an individual and collective responsibility to ensure respect for other people and property is maintained.

- Know that the use of mobile phones in lectures, seminars and computing laboratories is strictly prohibited. Mobile phones should be switched into silent mode before entering the secure area of the Learning Resource Centre.

- Know that the Studio will not tolerate antisocial behaviour: this includes the use of abusive language, physical abuse, obscene comments, verbal or physical harassment and comments or remarks that discriminate on the basis of sex, race or any other irrelevant distinction

Penalties for Unacceptable Use

Infringements of this Policy will be dealt with within the Studio's normal disciplinary procedures.

Recording of Lectures

COLLECTIVE recognises that from time-to-time students may wish to record lectures, seminars and tutorials for their own personal use to support their learning. As a matter of courtesy students should inform the lecturer prior to the commencement of the recording. If the student has not informed the lecturer, the lecturer may ask for the recording to be stopped.

However, students are reminded that:

- Distributing a recorded lecture/seminar/tutorial is an unacceptable activity. Students should always check with lecturers before distributing a recording; this includes distributing on the internet

- Editing a recorded lecture/seminar/tutorial is also an unacceptable activity. Students should always check with lecturers before changing a recording

Publishing to the Web

The Studio provides the opportunity to publish web pages within the Collective.co.uk domain to:

- support research activity

- enhance teaching

- provide means of disseminating information about the Studio to its members, to potential staff and students and to the general public.

- allow individual users to provide non-academic information as part of the general process of learning through our use of Google sites and wikis

Guidelines

All information provided using our web facilities will be seen as having, in some way, the support of the Studio and will affect how people view the Studio. Therefore, no provider should publish any information in a way which could adversely affect the good name or reputation of the Studio, nor provide material which is inappropriate for dissemination by the Studio. Included in this is any material that could lead to legal action, such as alleged libel or a breach of copyright.

A disclaimer should also be included indicating that the Studio has no direct responsibility for the content and giving individual contact name and email address.

The information provided on this web page does not necessarily represent the views of Collective Acting Studio. The responsibility for all material in this page rests wholly on a personal basis with the owner of this page. The named owner of this page is responsible for liability for loss, liability for hypertext links, liability for defamation and for compliance with relevant acts of law.

Google sites and wikis

All of the above Guidelines apply to the Google sites/wikis service, except that contributions will in this case always be at the page level with automatic attribution made to the author, such that no further use of the copyright symbol, linking to any Home Page, or disclaimer is necessary.

11

The service is offered to certain members of the Studio either as part of their learning, research or other use considered appropriate by the Head of Information and Learning Services.

All information published on our web pages is subject to our standard takedown policy whereby any report of issues with content will result in the page being removed immediately and subject to investigation.

Policy Review

This Acceptable Use of IT Policy will be reviewed annually to ensure it remains current with technological advancements, legal requirements, and Studio needs. The next review is due 23 July 2025.

By using Collective Acting Studio's ICT resources, you agree to comply with this Acceptable Use Policy. If you have any questions or concerns, please contact the Operations department.