ART ACADEMY
LONDON

IT User Policy (full version)

---

1. Introduction

It is the responsibility of all users of the Art Academy's I.T. services to read and understand this policy.
This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.1 Purpose

This Acceptable Use Policy is intended to provide a framework for such use of the Academy's I.T. resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to. The purpose of the policy and associated rules is:

- To ensure proper usage;
- to reflect the Academy's regulations;
- to reflect UK laws and statutes.

2. Policy

This Acceptable Use Policy is intended to assist in the Academy's duty of care to its students as well as protect its facilities, data and services whilst complying to relevant laws such as the copyright, design and patents act.

The Art Academy has a statutory duty to fully comply with (and report on) Section 26 of the Counter Terrorism and Security Act 2015. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. The Prevent Policy outlines the Academy's responsibilities in relation to the Prevent duty and is embedded into a number of the Academy's policies, including this one, as part of our wider duty of care to both students and staff.

3. Scope

Members of the Academy and all other users (staff, students, visitors, contractors and others) of the Academy's facilities are bound by the provisions of its policies in addition to this Acceptable Use Policy. The Art Academy seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students and staff.

3.1 Personal use of facilities

Academy information and communication facilities, including email addresses and computers, are provided for academic and administrative purposes related to work or study at the Academy. Very occasional personal use is permitted but only so long as:

- It does not interfere with the member of staff's work nor the student's study;
- it does not contravene any Academy's policies;
- it is not excessive in its use of resources.

Academy facilities should not be used for the storage of data unrelated to membership of the Academy. In particular, Academy facilities should not be used to store copies of personal photographs, music collections or personal emails.

All use of Academy information and communication facilities, including any personal use is subject to Academy Policy.

3.2 Connecting devices to Academy networks

In order to reduce risks of malware infection and propagation and risks of network disruption it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the Academy's wireless networks.

3.3 Unattended equipment

Computers and other equipment used to access Academy facilities must not be left unattended and unlocked if logged in. Members must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended. Particular care should be taken to ensure the physical security of all equipment when in transit.

4. Unacceptable use

In addition to what has already been stated above, the following are also considered to be unacceptable uses of Academy facilities.

A) Subject to exemptions defined in 2.1, the Academy Network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

1. Any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited "nuisance" emails;
4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Academy or a third party;
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party;
9. material that brings the Academy into disrepute;
10. material that contravenes the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulations (GDPR).

B) The Academy Network must not be deliberately used by a user for activities having, or likely to have, any of the following characteristics:

1. Intentionally wasting staff effort or other Academy resources;
2. corrupting, altering or destroying another User's data without their consent;
3. disrupting the work of other users or the correct functioning of the Academy Network; or
4. denying access to the Academy and its services to other users;
5. pursuance of commercial activities (even if in support of Academy business), subject to a range of exceptions. Contact the Operations Manager to discuss your commercial need.

C) Where the Academy Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Academy Network.

D) Users shall not:

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

4.1 Exemptions from Unacceptable Use.

There are a number of legitimate academic activities that may be carried out using Academy information systems that could be considered unacceptable use, as defined at 2A-D.

For example, research involving defamatory, discriminatory or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques. In such circumstances advice should be sought from the Director of Academic Quality, Standards & Student Experience (if potentially illegal material is involved). The Director of Academic Quality, Standards & Student Experience should also be notified if the material relates to the promotion of extremism/terrorism prior to the introduction of said material onto the Academy network.

Any potential research involving obscene or indecent material must always be discussed in advance with the Director of Academic Quality, Standards & Student Experience.

If a member of the Academy community believes they may have encountered breaches of any of the above, they should make this known to the Director of Operations.

5. Consequences of Breach

In the event of a breach of this IT User Policy by a User the Academy may in its sole discretion:

a) Restrict or terminate a User's right to use the Academy Network;
b) withdraw or remove any material uploaded by that User in contravention of this Policy; or
c) 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.

In addition, where the User is also a member of the Academy community, the Academy may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Regulations.

6. Definitions

Academy Network – all computing, telecommunication, and networking facilities provided by the Academy, with particular reference to all computing devices, either personal or Academy owned, connected to systems and services supplied.

Policies and documents that supplement and reference this document:

Student Handbook
Tutor Handbook
Staff Handbook
Moodle guide
Freedom of Speech Policy
PREVENT Policy
Safeguarding Policy
Disciplinary Policy and procedure
Data Protection Policy
Information Security Strategy

Document name	IT User Policy	Document owner	Harriet Wheeler & Darren Nairn
Date originally created	Dec 2016		
Version	3	Review date	May 2021
Author of amendments	Darren Nairn	Next review date	May 2025
Changes (list sections)	4.1		
Approved by	Board of Trustees	Date of approval	May 2021