POLICY 018

ACCEPTABLE USE OF IT AND E-SAFETY

Not a controlled document when printed

If you have a disability which makes reading this document or navigating our website difficult and you would like to receive information in an alternative format, please contact: and@acm.ac.uk

Policy 018: Acceptable Use of IT and E-safety

1. Purpose and Scope

1.1 This policy describes how the Academy of Contemporary Music (ACM) looks upon the issue of the Acceptable Use of IT and E-Safety. It covers the issue of the safety of students, staff and potentially other individuals using the internet and electronic communication devices such as email, mobile phones, games consoles and social networking sites, whether using ACM systems or devices of their own.

1.2 This policy applies to all computer users ('Users') within ACM (including persons who are not staff or students but who have been authorised to use ACM's IT facilities) whether they use IT equipment based at ACM's premises or access the systems provided by ACM via the internet using ACM-owned or private computing equipment. Compliance with this policy does not imply authorisation to use ACM's facilities.

1.3 This policy is designed to ensure that all are treated in a fair and equitable manner.

1.4 This policy covers:

- The use of all ACM IT facilities and systems, which include the local area network (LAN); any other directly or indirectly connected network; and the internet.
    - (b) The production of any material using ACM IT facilities, including printed output, internet pages, email messages and social media.
    - (c) The publication of any material relating to ACM systems within and outside of ACM.

1.5 The content of this policy aligns with government legislation, the regulations of ACM's validating partners and other external stakeholders to whom ACM must make reference.

2. Policy Statement

Acceptable Use of IT and E-safety

2.1 ACM recognises the key role that IT plays in supporting both the educational and business administration needs of the company. ACM is committed to ensuring that both staff and students have access to the necessary facilities and support, and remain safe while using them.

2.2 ACM's IT facilities are provided to assist with day to day work or studies. Use for any other purpose is only by concession and should be strictly limited with utmost care taken to ensure that nothing is done that will interfere with operations.

2.3 When using ACM's IT facilities users must conduct themselves, at all times, in a

lawful and appropriate manner so as not to discredit or harm ACM or other users and at all times in accordance with the contents of this policy. Accordingly, this policy is not a definitive statement of the purposes for which ACM's IT facilities should or should not be used and ACM reserves the right to apply this policy in a purposive manner.

2.4 ACM reserves the right to place whatever limitations it deems appropriate on usage in order to safeguard the function of its IT facilities and users' compliance with any applicable laws and/or the contents of this policy.

2.5 The breadth of issues classified by Ofsted as falling within e-safety is considerable, but can be categorised into three areas of risk:

- (a) content: being exposed to illegal, inappropriate or harmful material
- (b) contact: being subjected to harmful online interaction with other users
- (c) conduct: personal online behaviour that increases the likelihood of, or causes harm

2.6 ACM considers students' e-safety to be the responsibility of all members of ACM staff as well as that of ACM students.

2.7 Staff members must do all that they reasonably can to ensure that social media environments are safe for staff and students, and act accordingly if privacy issues, abuse or bullying take place. For further information about how ACM staff and students are expected to behave on social media, please refer to the ACM Social Media Policy and Procedures.

2.8 ACM ensures that the network is safe and secure. ACM ensures that security software up to date and fit for purpose. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers and workstations to prevent malicious or accidental access of ACM systems and information. On occasion, and where deemed necessary to do so, digital communications, including emails and internet postings, over the ACM network, will be monitored in accordance with this policy.

2.9 Monitoring of internet is undertaken to ensure that there are no breaches, or threats to ACM networks.

2.10 Failure or refusal to comply with this policy is considered to be a serious disciplinary offence which may lead to disciplinary action including, without limitation, withdrawal of services, expulsion/dismissal (with or without notice) and/or referral to the relevant authorities.

2.11 ACM will report any illegal or suspicious activity to the relevant external agencies and work in collaboration with these agencies to ensure that any risks are managed effectively through implementation of proportionate measures. This extends to the accessing, and distribution, or promulgation of any illegal or offensive materials and/or communications that may seek to victimise, cause offensive, radicalise or vilify any individual or organisation. This extends to sharing of, distribution, and communication of any extremist materials and communications in accordance with the Prevent Duty and association provisions.

3. **Responsible Parties**

3.1 The policy lead is responsible for the cyclical monitoring and review of the policy in liaison with the Quality Assurance and Enhancement Manager. The Acceptable Use of

IT and E-Safety Policy lead is:

- Head of Information Technology

3.2 Decisions and appropriate actions in support of the implementation of the Policy will be authorised by the following designated staff:

- Head of Information Technology
- Human Resources Manager
- Head of Education
- Pathway Leaders

4. Reference Points

4.1 Internal:

- Academic Appeals
- Academic Integrity
- Bullying & Harassment Policy
- Equality & Diversity Policy
- Safeguarding Policy
- Staff Social Media Policy
- Data Protection Policy
- Student Disciplinary Policy
- Student Complaints & Grievances Policy

4.2 External:

- Data Protection Act 1988 and 2003
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Freedom of Information Act 2000
- Ofsted Inspecting E-Safety Guide
- Preventing and Tackling Bullying (Department of Education)
- Childnet International Staff E-Safety Guidance
- The Prevent Duty
- Ofsted Inspecting e-safety guide (published April 2014 and withdrawn July 2014)

5. Date of Approval and Next Review

Version: 1.2

Approved on: 15 Sep 2022

Approved by: HR Executive

Next Review: Aug 2023