E-Safety Policy and Procedure

Version	**1.0**
Effective date	**June 2015**
Date for review	**January 2016**
Policy owner	**Director of Marketing, IT and Communications**
Reference points	**Ofsted Inspecting E-Safety Guide; Preventing and Tackling Bullying (Department of Education); Childnet International Staff E-safety guidance;**
Audience / handling notes	**Public**
Dissemination and implementation plan	This E-Safety policy will be published on the My ACM area of the ACM website for reference by students, staff and all other stakeholders. Heads of School will be informed by email that this policy and procedure has been agreed and directed to where it is published. Heads of School will be responsible for the dissemination of the policy and procedures to academic staff; the Director of IT, Marketing and Communications will be responsible for the dissemination of the policy and procedures to support staff. Students will be informed by email that this information has been updated and is available on the ACM website. ACM students will also be offered training in e-safety during induction activities.
Approving Committee	**Policy and Strategy Committee**
Date approved	

Version	Date	Activity

Initial Equalities Impact Assessment (EIA) Questions for ACM Policies:

Equality Impact Assessments (EIA) are a legal requirement of public bodies and form part of the specific duties on universities and colleges to help them meet their general equality duties. For more information on EIA, please refer to the ACM Equality and Diversity Policy.

An EIA involves gathering and using evidence to make a judgement about how a particular policy or practice affects, or is likely to affect, protected equality groups of people when it is implemented. Protected groups[1] are identified in the Equality Act 2010 as sharing a particular characteristic against which it is illegal to discriminate. The assessment should identify whether the policy and its related procedures affect people from different equality strands in different ways and if they do then it should establish whether the differential impact is positive, negative or neutral.

This form is intended to provide a quick assessment of whether a policy requires a Full EIA. It is also intended to be used to EIA all new policies.

a) Is there any aspect of the policy, procedure or practice that is likely to have a differential impact (negative or positive) on any of the protected characteristics?

☒ No
☐ Yes

If yes, identify how the impact would affect the specific equality strand:

b) Is there a possibility of unlawful discrimination, directly or indirectly, on any of the protected characteristics?

☒ No
☐ Yes

c) Could there be an effect on relations between certain groups?

☒ No
☐ Yes

d) Can the above differences be justified?

☐ No
☐ Yes
☒ N/A

e) What mechanisms are in place to monitor the application of the policy, procedure or practice across people from all protected equality groups? Please explain:

The impact of the policy will be reviewed bi-annually due to the rapid advances in new technologies. The policy will also be considered should there be any concerns raised by the Safeguarding Team or Senior Management Team or where an e-safety incident has been reported to and recorded by the Marketing, IT and Communications Department.

[1] The nine protected groups are defined in the ACM Equality and Diversity Policy. In brief, they are: Age; Disability; Gender re-assignment; Marriage and civil partnership; Pregnancy and maternity; Race; Religion and belief; Sex; Sexual orientation.

E-Safety

1. Policy Statement

1.1. This policy describes how the Academy of Contemporary Music (ACM) looks upon the issue of the safety of students using the internet and electronic communication devices such as email, mobile phones, games consoles and social networking sites, whether using ACM systems or resources of their own.

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

1.3. The Director of Marketing, IT and Communications is responsible for managing and reviewing this policy and the IT Department is responsible for the effective operation of the E-Safety Policy outlined below.

1.4. 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.

1.1. The E-Safety policy has a link with the following policies and procedures:

- Acceptable Use of Information Technology
- Bullying and Harassment
- Equality and Diversity
- Safeguarding
- Social Media
- Student Complaints & Grievances
- Student Disciplinary

2. Objectives

2.1. To explain in an open, transparent and accessible way how ACM views the safety of its students when using the internet.

2.2. To recommend steps which students can employ to maintain their safety when using the internet and other technologies.

3. E-Safety

3.1. 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 doing so.

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

3.2.1. content: being exposed to illegal, inappropriate or harmful material
3.2.2. contact: being subjected to harmful online interaction with other users
3.2.3. conduct: personal online behaviour that increases the likelihood of, or causes, harm.[1]

[1] Ofsted Inspecting e-safety guide (published April 2014 and withdrawn July 2014)

Further examples of risks in these areas can be found in appendix 1.

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

3.4. 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.

4. **Security:**

4.1. ACM will do all it can to ensure that the network is safe and secure. Every effort will be made to keep 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, work stations to prevent malicious or accidental access of ACM systems and information. Digital communications, including emails and internet postings, over the ACM network, will be monitored in accordance with the Acceptable Use of IT Policy.

4.2. Internet usage and monitoring is in place, use of accounts that are password protected enable detailed monitoring to take place, and users also have their own storage and e-mail accounts that are also subject to monitoring.

5. Student Behaviour:

5.1. ACM students are required to:

5.1.1. Be responsible for using ACM's IT facilities in accordance with the Acceptable Use of IT Policy;
5.1.2. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
5.1.3. Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
5.1.4. Understand the importance of adopting good e-safety practice when using digital technologies and realise that ACM's E-Safety Policy covers their actions outside of the ACM site if related to their membership of ACM.

5.2. When students enrol at ACM they sign an agreement regarding their safe and proper use of the internet and other technologies. Students thereby agree to follow the rules outlined below. ACM expects this behaviour of each student in order to maintain the safety and well-being of all students:

DO NOT:

- Share your passwords, personal information or location during online activity as this could have unwanted results, including theft of your identity;
- Agree to meet anyone you have only 'met' online;
- Engage in any communication of a sexual nature – either by phone text ('sexting'), email, social media or any other form of internet based communication;

- Expose yourself to inappropriate content, websites or images, even just out of curiosity;
- Expose yourself or others to any content promoting hate, discrimination or violence;
- Illegally download any copyrighted content – including music, video, games and applications;
- Engage in any illegal online activity – including hacking, financial scams, spreading viruses/ malicious software or creating / uploading inappropriate material;
- Spend long periods online without taking a break. Every hour or so move around and give your eyes a rest.

DO:

- Conduct yourself online in a professional and responsible manner; be mindful of how you present yourself in the digital domain;
- Be considerate of other users.
- Remember that once it's out there, you cannot get it back. Who is looking at all the personal information you are freely giving away? Think before you share;
- Beware of in-app purchasing and financial scams which could result in your financial risk;
- Remember that strangers can hide behind false identities – that A&R man offering you a record deal may not be who he seems to be. If in any doubt please contact the ACM Industry Link Team via industrylink@acm.ac.uk;
- Remember that visiting certain sites may result in the police visiting you!

6. Plagiarism and Copyright

6.1. Students should be encouraged to question the viability and reliability of materials researched, viewed or downloaded. They should be encouraged to respect the copyright of other parties and to cite reference properly.

For more information students should refer to the 'Harvard Referencing Guide' available in the 'Dissertation Guides' section of the MyACM area of the ACM website.

6.2. For further information about the use of other peoples' material on social media please refer to the ACM Social Media Policy and Procedures.

7. Cyber-bullying

7.1. Cyber-bullying is a form of bullying which utilises technology. It can happen at all times of the day, with a potentially bigger audience, and more accessories as people can quickly and easily forward on content. The rapid development of, and widespread access to, technology has assisted cyber-bullying and as such it is difficult to police.[2]

7.2. The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones. Advice on teachers' powers to search (including statutory guidance on dealing with electronic devices) is available from:

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

[2] Preventing and Tackling Bullying: Advice for Headteachers, Staff and Governing Bodies, October 2014, p.6

7.3. Members of staff should refer to ACM's Bullying & Harassment Policy and Procedures to address any allegations of bullying.

7.4. Anyone found guilty of cyber-bullying will face disciplinary action under ACM's Student Discipline Policy and Procedures.

8. Extremism & Radicalisation Websites

8.1. "Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. Calls for the death of members of British armed forces is also included in this definition." (*Prevent,* Police & Schools Association of Chief Police Officers (ACPO) 2013).

8.2. Under the Counter-Terrorism and Security Act 2015 ACM staff have a duty to have due regard to the need to prevent students and staff from being drawn into terrorism, including travelling to join/support terrorist groups.

8.3. ACM keeps its students safe from terrorist and extremist material by setting appropriate levels of filtering on the internet when accessed via ACM IT facilities.

8.4. If ACM staff are concerned that students have been visiting websites that may be affecting students' views and behaviour, they should contact Registry via registry@acm.ac.uk who will advise on next steps.

9. Procedure for Reporting an E-Safety Incident

9.1. ACM takes students' online safety very seriously. Students who have worries about any aspects of their e-safety, or that of another ACM student are advised to contact their mentor, another tutor, IT via ITSupport@acm.ac.uk or ACM's Designated Safeguarding Lead via safeguarding@acm.ac.uk. ACM will ensure the concern is quickly and appropriately addressed.

9.2. When contacting the appropriate department, please detail the following:

i. **When** (dates/times);
ii. **Where** (places);
iii. **Who** (any names of participants in the transgression);

plus

iv. Names of any witnesses;
v. Any action taken, e.g. reported to a member of staff;
vi. Original copies of any correspondence or written material connected with the issue.

9.3. ACM will act immediately to prevent, as far as is reasonably possible, any harm or further harm occurring.

9.4. Staff should take care not to guarantee any measure of confidentiality to any individual reporting any concerns regarding e-safety.

9.5. Following any reported incident a full investigation will be carried out and ACM will decide on the most appropriate course of action. Depending on the seriousness of the incident, actions may include:

9.5.1. withdrawal of services;
9.5.2. expulsion or dismissal;
9.5.3. involvement of external agencies, such as the police.

10. More Serious Student Safety Concerns

10.1. If ACM staff have a more serious concern about the safety of a student, they should report their concerns to a member of the ACM Safeguarding Team. There will always be a member of the designated safeguarding team on duty to respond to any allegations/ suspicions/ concerns of abuse.

10.2. The ACM Safeguarding Team are:

- **Designated Safeguarding Leads (DSLs) Fiona Lambie –** Senior Specialist Tutor and Wendy Finlay – Registrar
- Helen Hosker – Specialist Tutor
- Karen Kirk – Assistant Registrar (Student & Programme Administration)
- Rosita Vazquelero – Student Administration Officer
- Roger Davis – Part-Time School Manager
- Adam Pain – Senior Lecture
- Jo MacKinnon – Head of Mentoring
- Matt Bates – E-Safety Officer

You can contact any of the members of the team via:

- safeguarding@acm.ac.uk; or
- ACM switchboard number: 01483 500800

10.3. For more information about Safeguarding, members of staff should refer to ACM's Safeguarding Policy and Procedures.

Appendix 1:

Common E-Safety Risks

Content

- exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); and substance abuse
- lifestyle websites, for example pro-anorexia, self-harm or suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content.

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film).