Acceptable Use of Information Technology Policy

Version	**1.1**
Effective date	**June 2016**
Date for review	**September 2016**
Policy owner	**Registrar**
Reference points	**Guildford College Equality and Diversity Policy, Middlesex University Regulations, Prevent Duty**
Audience / handling notes	**Public**
Dissemination and implementation plan	This Acceptable Use of Information Technology 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 Registrar and 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.
Approving Committee	**Policy and Strategy Committee**
Date approved	**26.5.16**

Version	Date	Activity
1.1	25.5.16	Updated to reflect Prevent Duty

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:

Registry will record the number and type of incidences of misuse of ACM's IT facilities in an academic year in order to identify trends, evaluate the effectiveness of and make enhancements to the Acceptable Use of IT Policy.

[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.

Acceptable Use of Information Technology (IT)

1. Policy Statement

1.1. This policy describes how the Academy of Contemporary Music (ACM) looks upon the issue of the Acceptable Use of IT.

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 in writing by ACM 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 both are treated in a fair and equitable manner.

1.4. This policy covers:

1.4.1. 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.

1.4.2. The production of any material using ACM IT facilities, including printed output, internet pages, email messages and social media.

1.4.3. The publication of any material relating to ACM systems within and outside of ACM.

1.5. The Director of Marketing, IT and Communications is responsible for managing and reviewing this policy and IT staff are responsible for the effective operation of the Acceptable Use of IT Policy and Procedures outlined below.

1.6. 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.

1.7. The Acceptable Use of IT Policy has a link with the following policies and procedures:

- Academic Appeals
- Academic Misconduct
- Bullying and Harassment
- Equality and Diversity
- E-Safety
- Safeguarding
- Social Media
- Student Disciplinary
- Student Complaints & Grievances

2. Objectives

2.1. To explain in an open, transparent and accessible way how ACM deals with students' use and misuse of ACM IT facilities and applications.

2.2. To describe:

- how Users or ACM may be liable in law for misuse of the ACM's IT facilities and applications;
- how Users' interests and ACM's interests can be protected;
- how to report abuse, misuse or access to inappropriate materials;
- the action which may be taken against Users if they fail to comply with the rules and regulations set out in this policy.

3. Acceptable Use of IT

Summary of Items Following in this Policy:

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.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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.

3.6. ACM reserves the right to amend any of the rules set out in this Policy at any time, and will notify all staff and students of any changes it makes.

4. Procedure for reporting abuse, misuse or access to inappropriate materials

4.1. If students or staff become aware of any transgressions of the Acceptable Use of IT Policy, they should contact the most appropriate of the following departments via the email address below:

4.1.1 IT: ITSupport@acm.ac.uk
4.1.2 Safeguarding: safeguarding@acm.ac.uk
4.1.3 Human Resources: HR@acm.ac.uk
4.1.4 Registry: registry@acm.ac.uk

4.2 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.

4.3 ACM will ensure the concern is quickly and appropriately addressed.

5 Basic Rules

5.1 Only use ACM's IT facilities for lawful activities. ACM will not hesitate to contact the police if it discovers unlawful use of ACM's IT facilities.

5.2 Do not engage in any activity or omit to do anything which could jeopardise the integrity or security of ACM's IT facilities.

5.3 Keep your 'Network Identity', each of your User 'Accounts' and associated passwords secure.

5.4 Do not share your own or use someone else's 'Network Identity' and User Account.

5.5 Do not use, or permit others to use, ACM's IT network for any commercial use, nor for the purposes of endorsing or advertising such activity without the express authority of ACM's IT Department.

5.6 Do not alter, interfere, add to or remove any physical part of ACM's IT facilities or any equipment connected or attached to the University's computing facilities without authorisation. Data points provided for Users are designed to support one computer only and the unauthorised connection of hubs and switches to data points is forbidden.

5.7 Do not access material, or attempt to access material, that you do not have permission to access.

5.8 Do not bypass the login procedure.

5.9 Do not deny (or do anything which has the effect of denying) another Users' legitimate access to ACM's IT facilities.

5.10 Do not connect any server, modem, wireless routers and hubs or network routers / switches / hubs to ACM's IT network, or other similar transmitting device that operates on a wireless frequency without prior written agreement from the IT Department.

5.11 Do not make, store or transmit unlicensed copies of any trade mark or copyrighted work (including software and media files).

5.12 Do not send unsolicited bulk email messages, chain mail or spam.

5.13 Do not deliberately or recklessly undertake activities which may result in any of the following:

- The waste of staff effort or network resources, including time on any system accessible via ACM's IT network;
- The corruption or disruption of other User's data;
- The violation of the privacy of other Users;
- The disruption of the work of other Users;
- The introduction or transmission of a virus into the network.

6 E-mail

6.1 ACM encourages Users to use email as a prompt and effective method of communication.

6.2 Users must act responsibly and appropriately when using ACM's IT facilities to send email, whether internally or externally using the Internet.

6.3 No User should send any email that contains any material that ACM considers or might reasonably be considered by the recipient to be bullying, harassing, obscene, racist, sexist, defamatory, offensive, "chain mail", incitement to commit a criminal offence or threatening or which contains any malicious code; for example a virus. If you receive an email containing any such material, and you are concerned about this you should inform your relevant Pathway Leader or Manager of Service.

6.4 Users must not send email which might bring ACM into disrepute or purport to be the view(s) of ACM unless the User is authorised in writing to express views on behalf of ACM.

6.5 ACM and ACM on behalf of its externally hosted providers, reserves the right to automatically delete emails which are found to contain viruses. ACM endeavours to protect Users from offensive emails through the operation of 'Anti Spam filters' PROVIDED THAT in addition, Users endeavour to reduce the amount of offensive material they receive by the configuration of their email setup to screen out and delete unwanted emails.

6.6 Users hereby agree that emails generated by, or stored on, ACM's computers may be subject to disclosure under the Freedom of Information Act and Data Protection Act as well as potentially disclosable and admissible in evidence, in a dispute.

7 Unauthorised Use of the Internet

7.1 Do not, other than for ethically cleared, properly approved and lawful research purposes (as set out below) visit, view, store, download, transmit, display, print or distribute any material relating to:

7.1.1 Sex or pornography;
7.1.2 Lewd or obscene material of any nature or other material which may be likely to cause offence to another person;
7.1.3 Terrorism or cults;
7.1.4 Hate sites (racial or other).

Users seeking authorisation should obtain prior written approval from the appropriate Module Leader or Line Manager, (and this approval needs to be reconfirmed in writing every 6 months). In addition, Users should not intentionally do anything which enables others to visit, view, download transmit, display, or distribute any material relating to the items listed above.

7.2 Do not attempt to gain unauthorised access to any facility or service within or outside ACM, or make any attempt to disrupt or impair such a service.

7.3 Do not set up or use hardware, or software, on ACM's own internal network for the purpose of sniffing, hacking, network scanning or keyboard logging without prior written authorization.

7.4 Do not alter or interfere with data, programs, files, electronic mail or other computer material which you do not have the right to alter.

7.5 News Groups, Web Sites, Wikis, Blogs:

7.5.1 Do not post or present information in such a way as may bring ACM into disrepute or otherwise damage ACM's reputation.

7.5.2 Do not express opinions which purport to be ACM's view unless you are authorised in writing to express views on behalf of ACM.

7.6 Any transgression or breach of the above restrictions or policies will be deemed as gross misconduct and/or a serious offence which may result in withdrawal of services and/or expulsion or dismissal following a proper hearing of the case. Users will be held responsible for any claims brought against ACM in respect of any legal action to which ACM is, or might be, exposed as a result of User's misuse of ACM's IT facilities, including reimbursing ACM for any financial liability which ACM suffers as a result of a User's actions or omissions. ACM will not hesitate to contact the police if it discovers unlawful use of ACM's IT facilities.

8 Unintentional Access to Inappropriate Internet Sites

8.1 ACM accepts that mistakes can be made due to unintended responses of search engines, unclear hypertext links, misleading advertisements and typing errors taking Users to inappropriate web pages.

9 Legitimate Use

9.1 There may be circumstances where a User feels that the nature of their work or studies means they have a legitimate reason for accessing and/ or using material prohibited under this Policy. In this circumstance the User must discuss this with their Pathway Leader (students) or line manager (staff) in advance as to the precise reasons for such access and use and no such access and/or use may be undertaken without the express written approval of the Pathway Leader/ line manager. If the Pathway Leader/ line manager is in doubt they must contact the IT Department for advice.

10 Software

10.1 **Unauthorised Software:**
ACM will take disciplinary action against any User who acquires, uses or distributes unauthorised copies of any software using ACM's IT facilities.

10.2 **Introducing Software:**
Users are prohibited from using any software on ACM's IT facilities which the User and/or ACM is not licensed to use.

10.3 Even if a software product has been properly purchased and licensed, it must not be installed on any PC or Mac without prior approval of the IT department.

10.4 **Educational Use Licences:**
ACM licenses computer software from a variety of outside sources and many software packages are licensed only for educational use. ACM does not own this software or related documentation and, unless authorised by the software owner, does not have the right to reproduce it. The software used on the LAN or multiple/individual machines may only be used in accordance with the relevant licence agreement and in no circumstances for any commercial use without the express authorisation of the IT Department.

10.5 **Distribution of Software:**
Users are prohibited from using ACM's IT facilities to distribute software unless (and not without ACM's express written approval) it is directly associated with the ACM's

business and where such distribution does not contravene any other part of this Policy.

10.6 **Suspected Misuse:**
Users should immediately notify the IT Department of any misuse or suspected misuse of software or associated documentation.

10.7 **Online Plagiarism and Online Purchasing of Assignments:**
ACM is aware of online plagiarism and that sites exist where it is possible to purchase assignments. Users hereby acknowledge and agree that ACM actively monitors Internet use and submitted assignments for evidence of plagiarism. Any abuse or evidence of plagiarism is considered to be a serious offence, and will be dealt with under Academic Misconduct procedures.

11 Security and Viruses

11.1 It is each User's responsibility to log off from the system when leaving the computer being used to avoid inadvertent security breaches.

11.2 Users must not disclose (including by sending via or placing on the Internet) any material, which incites or encourages or enables others to gain unauthorised access to ACM's IT facilities.

11.3 It is vital that all Users take all necessary steps to safeguard ACM's IT facilities from viruses. Accordingly, all Users using personal computers on ACM's network must ensure that anti-virus software is installed on their desktop / laptop computer and kept up to date and that any unsolicited documents or attachments received are deleted immediately.

12 Offensive or Defamatory Material

12.1 Emails and the Internet are considered to be a form of publication and therefore the use of the Internet, email and the making available of any information online, must not be offensive, (including without limitation bullying, harassing, discriminatory, pornographic, homophobic, excessively violent, obscene, blasphemous, seditious, incite racial hatred), defamatory or in any way break any law relating to published material. Misuse of email or inappropriate use of the Internet by viewing, accessing, transmitting or downloading any such offensive information will amount to a serious offence and/or gross misconduct and may result in withdrawal of services, expulsion/dismissal or other penalties.

12.2 Words and pictures produced on the Internet are capable of being defamatory if, for instance, they are untrue, ridicule a person and as a result damage that person's reputation. For these purposes, as well as any individuals, a "person" may include ACM or another institution. You must not create or transmit any statement which may be offensive or defamatory in the course of using the Internet or ACM's IT facilities whether in emails or otherwise. As well as you being personally exposed to potential legal action for defamation, ACM as the 'Internet Service Provider' would also be held liable.

13 Obscenity

13.1 It is a criminal offence to publish or distribute obscene material or to display indecent material in public. The Internet or any computer 'message boards' qualify as a public place. The accessing or sending of obscene or indecent material using ACM's IT facilities is strictly forbidden and may result in withdrawal of services or expulsion/dismissal.

14 Discrimination and Harassment

14.1 ACM does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed on ACM's IT facilities or via the Internet. Users should not view, use or distribute any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability.

15 Extremism & Radicalisation

15.1 "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 are also included in this definition." (*Prevent,* Police & Schools Association of Chief Police Officers (ACPO) 2013)

15.2 Prevention of radicalisation – the "Prevent" duty under the Counter-Terrorism and Security Act 2015 places a duty on ACM staff to have due regard to the need to prevent students and staff from being drawn into terrorism, including travelling to join/support terrorist groups. If a student is deemed vulnerable to being drawn into terrorism, support will be provided (in partnership with the local authority Channel panel).

Please refer to Appendix 1 for details regarding the Prevent Duty.

16 Data Protection

16.1 Any work involving processing, storing or recording personal data (information on an identifiable living individual) is governed by the Data Protection Act 1998. It is the User's responsibility to ensure that personal data is collected and used in accordance with the Act. Further information can be found in ACM's Data Protection Policy. If Users believe that their work involves the processing, storing or recording of personal data, Users must first obtain confirmation from the Academic Registrar that consent to such processing, storage or recording has been obtained.

17 Monitoring

17.1 ACM reserves the right without notice to monitor Users' use of ACM's IT facilities and to access data held on ACM's IT facilities for justifiable business purposes and in order to perform various legal obligations including:

17.2 where it is suspected that a User is misusing ACM's IT facilities;

17.3 to investigate misuse of ACM's IT facilities;

17.4 where ACM has received a request from an authorised external party to monitor a User's use of ACM's IT facilities;

17.5 to prevent or detect crime (including 'hacking');

17.6 to resolve system performance problems which may otherwise damage the computing services provided to other ACM users; or

17.7 to intercept emails for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding emails to correct destinations.

17.8 ACM reserves the right to automatically block certain network protocols and sites in order to minimise the risk of viruses, hacking, network scanning and other inappropriate file transfer activities.

17.9 ACM maintains logs of user and network activity which may be used in investigations of breaches of ACM's IT regulations, performance monitoring or provision of statistical reports.

17.10 ACM reserves the right to make and keep copies of emails and data documenting use of email and/or the Internet systems, for the purposes set out above.

17.11 Users hereby acknowledge and agree that ACM has the right to retain copies or delete copies of any data stored on the system so as to comply with ACM's statutory obligations or, at its own discretion, in accordance with the legitimate purposes stated above.

17.12 In using ACM's IT facilities, Users implicitly accept this Policy. Consequently Users agree to their activities being monitored in the circumstances given above.

18 Availability

18.1 Users acknowledge that ACM's IT facilities may not be available for 24 hours 7 days a week. ACM retains the right to limit or prevent access to ACM's IT facilities for the purposes of carrying out planned or unplanned maintenance, virus monitoring and/or clean up or investigation. Except where ACM cannot exclude or limit its liability as a matter of law, ACM shall have no liability to any User in connection with the non-availability of ACM's IT facilities howsoever arising, including in negligence.

19 Liability for Misuse and Disciplinary Action

19.1 Civil and Criminal Liability:
Users and ACM are potentially at risk for a range of civil and criminal liability arising from misuse of ACM's IT facilities. Legal liability can arise from:

- defamation under the Defamation Act 2013;
- copyright infringement under
    - the Copyright, Designs and Patent Act 1988;
- breach of confidence;
- negligent virus transmission;
- breach of the Computer Misuse Act 1990;
- breach of
    - the Obscene Publications Acts of 1959 and 1964;

  - the Protection of Children Act 1978;
  - the Telecommunications Act 1984;
  - the Communications Act 2003;
- computer hacking;
- harassment and discrimination under:
  - the Sex Discrimination Act 1975;
  - the Race Relations Act 1976;
  - the Disability Discrimination Act 2005;
  - the Equality Act 2010;
  - the Employment, Equality (Religion or Belief) Regulations 2007;
  - the Employment, Equality (Sexual Orientation) Regulations 2007;
  - the Racial and Religious Hatred Act 2006;
- the Data Protection Act 1998 and the Human Rights Act 1998;
- the Regulation of Investigatory Powers Act 2000.
- the Counter Terrorism and Security Act 2015

19.2 Misuse of ACM's IT facilities (including failing to comply with this Policy) may expose both Users personally and/or ACM to court proceedings attracting both criminal and civil liability. Users will be held responsible for any claims brought against ACM for any legal action to which ACM is, or might be, exposed as a result of User's misuse of ACM's IT facilities including reimbursing ACM for any financial liability which ACM suffers as a result of Users actions or omissions.

19.3 ACM considers failure or refusal to comply with this Policy to be a serious disciplinary offence which may lead to disciplinary action taken including withdrawal of services and/or expulsion/dismissal with or without notice. Action (including certain penalties) may be taken under ACM's Student Disciplinary Policy.

19.4 Users acknowledge that it is their own responsibility to create and maintain 'back-ups' of any data. The back-ups taken by ACM are used for systems recovery purposes. Users hereby acknowledge and agree that it is not possible to recover any emails and files held on ACM's IT Facilities.

20 ACM's Liability to Users

20.1 ACM does not exclude its liability under this Acceptable Use of IT policy (if any) to Users:

- for personal injury or death resulting from ACM's negligence;
- for any matter which it would be illegal for ACM to exclude or to attempt to exclude its liability; or
- for fraudulent misrepresentation.

20.2 Except as provided above, ACM will be under no liability to Users whatsoever (whether in contract, tort (including negligence), breach of statutory duty, restitution or otherwise) for any injury, death, damage or direct, indirect or consequential loss (all three of which terms include, without limitation, pure economic loss, loss of profits, loss of business, loss of data, loss of opportunity, depletion of goodwill and like loss) howsoever caused arising out of or in connection the use of ACM's computing facilities.

20.3 This Policy is governed by the laws of England and Wales and is subject to the non-exclusive jurisdiction of the English Courts.

APPENDIX 1: Prevent Duty

1. Introduction: Legal Context and the Academy Approach

1.1. The Counter Terrorism and Security Act 2015 places a duty on all RHEBs (Relevant Higher Education Bodies) to have due regard to the need to prevent people from being drawn into terrorism. This legislation is given specific statutory force through the Prevent duty guidance for higher education institutions in England and Wales, referred to as the 'Prevent Duty'.

1.2. The underlying considerations adopted by the Academy in implementing the Prevent Duty are:

- a commitment to the safety and wellbeing of our staff and students and all who interact with the Academy, including not being victims of, or complicit with any activities linked to radicalisation;
- preserving equality and diversity as foundations of the Academy life, whilst ensuring these values are not threatened;
- supporting campus cohesion and harmonious relations across all parts of the Academy community;
- that the requirements described in this Policy are implemented in a proportionate and risk-based manner, relevant to the local context in which the Academy campus is based.

1.3. The legal definition of terrorism as defined in the Terrorism Act 2000 applies to the Prevent duty. The Academy acknowledges and upholds the position that the definition of terrorism in the Terrorism Act is broad, in describing it as "the use or threat of action which involves serious damage to property; or endangers a person's life; or creates a serious risk to the health and safety of the public or a section of the public; or is designed seriously to interfere with or disrupt an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious, racial or ideological cause."

1.4. Terrorism may take the form of extremist behaviour and acts. The statutory Prevent Duty Guidance defines extremism as "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 and calls for the death of members of our armed forces, whether in this country or overseas".

1.5. In accordance with this definition, the Academy considers that extremist ideologies, and those who express them, undermine the principles of freedom of speech and academic freedom.

1.6. HEFCE is the principal regulator of the Academy and has established a monitoring framework to assess compliance of all Higher Education Providers with the Prevent Duty. The Academy has a legal duty to provide reports and evidence of its compliance with the Prevent Duty to HEFCE, including serious issues which arise related to the Academy's Prevent responsibilities. HEFCE's role does not extend to investigating terrorism-related incidents on campus.