Royal Conservatoire of Scotland

Online Safety Policy

Document Revision History

Version No.	Version Date	Prepared By	Approved By	Summary
1.1	March 2016	Caroline Cochrane		RCS Online Safety Policy – including PREVENT Duty
1.2	April 2016	C. Cochrane/Ewan Hainey		Inclusion of appropriate reporting lines
1.3	May 2016	C. Cochrane/Ewan Hainey	CSMT Risk Management	Inclusion of CSMT comments

Introduction

The Royal Conservatoire of Scotland recognises the benefits and opportunities which new technologies offer, both to teaching & learning and to being an engaged and active citizen within the world. RCS provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. The Royal Conservatoire of Scotland also has a duty under the Counter-Terrorism and Security Act 2015, termed "PREVENT", to aid the process of preventing people being drawn in to terrorism.

Our approach is to implement appropriate safeguards within the Conservatoire while supporting staff and students to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This online safety policy should be read alongside other relevant Conservatoire policies including (but not limited to) the ICT Acceptable Use, Information Security, Dignity at Work & Study, Disciplinary and Child Protection Policies.

Policy Scope & Objective

The policy applies to the entire Conservatoire community who have access to the Conservatoires IT network, both on the premises and remotely: it applies irrespective of the owner of the devise used. Any users of the network must adhere to and sign a copy of the ICT Acceptable Use Policy. The Online Safety Policy applies to all use of the internet and all forms of electronic communication such as email, mobile phones, social media sites, professional networks, games consoles, chatrooms, video conferencing and web cameras. The objective of this policy is to explain in an open, transparent and accessible way how RCS views the safety of its community when using the internet and to recommend steps which users can employ to maintain their safety when using the internet and other technologies.

Online Safety

RCS recognises the key role that technology plays in supporting both our educational and business administration needs. We are committed to ensuring that both staff and students have access to the necessary facilities and support, and remain safe while doing so. The breadth of issues surrounding online safety is considerable, but can be categorised into three main areas of risk:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Staff and students have a responsibility to protect themselves and others by ensuring that they conduct their online activity and behaviours in an accountable and responsible manner. To that end, the following guidance should be followed at all times and in all situations:

DO NOT:

- Share your passwords, personal information, phone number 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.
- Send pictures online or over a mobile unless you know the person in real life. It is easy for people to take your pictures and alter them and send them on.
- Expose yourself to inappropriate content, websites or images, even just out of curiosity.
- Expose yourself or others to any content promoting hate, discrimination, extremism, terrorism 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.
- Use a webcam with people you don't know in real life: webcam images can be recorded and copied and also shared with other people.
- 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.
- Always think of your personal safety first when using ICT or your mobile phone: remember it is easy for anyone to lie about who they are online, so you can never really be sure about who you are talking to.
- Be considerate of other users.
- Use privacy settings when setting up social media accounts or groups. This is so people who you don't want to see your profile can't.
- 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
- Remember that visiting certain sites may result in Conservatoire action and in some cases Police action

Responsibilities & Reporting an Online Safety Incident

Concerns about online safety reported to a member of staff (or any concern that a member of staff has her/himself about a student or colleague) should be relayed immediately to the Head of Information Services, the Academic Registrar or any member of the Conservatoire's Senior Management Team. The matter will then be referred to the Conservatoire's Risk Management Group (as the Conservatoire's Prevent group). However, depending on the nature of the concern and the immediacy of the threat to student(s) and/or staff, action may be taken by the appropriate member of staff in advance of any consideration of the concern by the Risk Management Group in accordance with Conservatoire policies. Depending on

the nature of the concern, external agencies (including Police Scotland) may be involved. Upon hearing a report of an online safety incident, staff should take care not to guarantee any measure of confidentiality to any individual reporting any concerns regarding online safety.

The Conservatoire's primary concern in this matter is safeguarding our community to ensure our staff & students can operate in the digital world in a secure, safe, legal and responsible manner. The Conservatoire has a clear understanding of our responsibilities, including the need to ensure full academic freedom whilst having due regard for the welfare of our students, staff and visitors. The Conservatoire will always react in a proportionate and, where possible, supportive way to any issues that may arise in respect to online safety.

Feedback and Further Information

The Royal Conservatoire of Scotland welcomes all constructive feedback on this and any other Conservatoire Policy. Training and guidance on online safety will be part of the induction process for all new staff and students, and further briefings will be delivered periodically. If you would like further information on online safety, please contact Caroline Cochrane, Head of Information Services.