POLICY ON E-SAFETY FOR STUDENTS

Overview

The primary focus of e-safety is child protection. It is important that we recognise, however, that e-safety risks are posed more by behaviour and values online than the technology itself. Our overall approach must be to allow, not to restrict access to technology. We need to empower learners to develop safe and responsible online behaviour to protect themselves. The aim of this policy is to give details of what Studio Cambridge does to promote the safe use of communication and digital technologies by students, with reference to other policies and procedures that support safe use.

Advice to staff on appropriate e-safety procedures and use of IT is covered in the staff handbook.

E-Safety for students

Students under the age of 18 are given guidance on how to stay safe on-line in the Student Code of Conduct and in their student handbook.

Anti-Bullying – cyberbullying

Guidance and the consequences for students involved in Cyberbullying are to be found in the School's Anti-Bullying Policy.

Sanctions

The major aim of the E-Safety Policy is to promote safe and effective use of communication and digital technologies, however, should sanctions be required, the school's disciplinary procedure would be implemented.

Use of mobile devices and school computers

The school facilitates a Bring Your Own Device (BYOD) approach to technology, enabled by a robust Wi-Fi network. Those connecting devices to the network have to read the below information:

Wi-Fi and Computer Use Terms and Conditions

The code of conduct that applies to all activities on premises used by Studio Cambridge extends to online activities and behaviour in virtual environments. The same standards of respect, courtesy and tolerance for fellow students and staff are expected. Any type of bullying, harassment, attempts to embarrass, deceive or manipulate are unacceptable.

Codes of conduct specific to IT use:

- Nothing should be published online and no messages should be sent that the Company management would not also consider fully acceptable face to face in the real world. Opinions and comments about other members of the school community and the school itself are subject to the norms that govern school life in general.
- Viewing certain types of material such as racist, extremist, terrorist or pornographic texts or images is not acceptable. Content filters are in place on the Company's networks, but the dynamic nature of the internet means even the best filters cannot be guaranteed as 100% reliable, and in the last resort the responsibility lies with the user.
- Users must not attempt to download, install, modify or remove any software, bypass internet filtering systems, or place the system at risk of viruses through use of contaminated removable media.
- Downloading, sending or publishing material that violates copyright or data protection law is forbidden, as is copying other users' files without their express permission.
- Hardware must not be disconnected, adjusted, moved or unplugged without the permission of the IT staff.
- Users must not knowingly attempt to compromise the security of the system or take any actions that jeopardise the privacy of others. Impersonating another user by logging on with their credentials,

attempting to bypass security settings to gain access to restricted or personal files, and sending unsolicited material to other users are not allowed.

Advice given to students when using social media

If anything you have seen or read disturbs you, you should tell a member of the Studio Welfare team.

You should not:

- give personal information such as address or phone number to strangers
- use a 'nickname' that includes your personal name or your age
- believe everything you read online
- use webcams with strangers
- arrange to meet a stranger
- post personal photos in public areas
- accept or post insults in any form (text, photo or video)
- answer messages from unknown sources
- download inappropriate links.

Reviewed: Jan 2021 by LE, RE & RM
Next review due: Jan 2022