SupaJam Online Safety Policy

August 2020

(Next review date August 2021)

1. PRINCIPLES

1.1 - All students at SupaJam Education in Music and Media (The College) have access to a range of new technologies for communicating and collaborating. It is essential that all students are safe and the same principles should apply to the 'virtual' or digital world as would be applied to The College's physical buildings.

1.2 - E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

2. PURPOSE OF THIS POLICY

- To ensure that email is monitored within the realms of the Human Rights Act.
- To give responsibility for using the internet to the students and parents.
- To educate students and parents about the moral and legal principles of using the internet on and off of college premises.
- To safeguard the publishing of students' details.
- To protect students and staff against the risks and consequences of unacceptable use.

3. GUIDELINES

3.1 - Teaching and learning

3.1.1 - The internet is an essential element for education, business and social interaction. The College has a duty to provide students with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

3.1.2 - Internet use will enhance academic learning;

- Students will understand the necessity for college internet access to be designed expressly for student use but include filtering appropriate to the age and/or needs of our students.

- Teaching students internet use that is and isn't acceptable and giving clear objectives for internet use will promote safer use of the internet.

- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

3.1.3 - Students will be taught how to evaluate internet content;

- SupaJam will ensure that the use of information used from the internet by staff and by students complies with copyright law.

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3.2 - Managing Internet Access

3.2.1 - Safeguarding Online;

- In accordance with the guidelines provided from PREVENT training, all staff are mindful of the need to be alert to any potential radicalisation and should in the first instance report it to the Safeguarding Lead (or a member of the Senior Leadership Team in their absence) who will take the appropriate action. All resources and learning materials are quality assured to ensure that the potential for radicalisation is minimised. Full details on radicalisation will be found in our Preventing Radicalisation policy.

- Students, where appropriate, are encouraged to recognise and report inappropriate material to a member of staff.

- Students are not to use live chat rooms whilst in college.

- Sexting, sexual harassment, cyberbullying and any other forms of harassment or abuse will not be tolerated and will be referred to the Senior Leadership Team. Students will be educated in the signs of online abuse and will be encouraged to report any concerns they may have.

- Each student will be provided with individual login credentials to access the internet whilst at SupaJam Education in Music and Media. The College has the ability to monitor those logins and the activity whilst using the internet.

- Key staff will receive training in online safety to ensure students are kept safe when using online systems and services.

3.2.2 - Information system security;

- The College's ICT systems capacity and security will be reviewed regularly.

- Virus protection will be installed and updated regularly.

- The College's technical infrastructure is to be secure and systems are in place and monitored regularly to ensure that this is not open to misuse or malicious attack.

3.2.3 – Email;

- Students may only use approved external email accounts on The College system.

- Students must immediately tell a member of staff if they receive offensive email(s).

- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on college headed paper. This is to prevent data protection breaches as well as maintaining the safety of students.

- The forwarding of chain letters is not permitted.

- Students must check who sent the email before reading and report any emails they are unsure of.

3.2.4 - Social networking and personal publishing;

- Students will be advised never to give out personal details of any kind which may identify them or their location.

- Students must not place personal photos on any social network space owned by SupaJam Education in Music & Media or affiliated companies without the explicit consent of the CEO's David Court and Nick Stillwell.

- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.

3.2.5 - Managing filtering;

- The College will work in partnership with the Local Authority, Department for Education and the internet Service Provider to ensure systems to protect students are reviewed and improved.

- If staff or students discover an unsuitable site, it must be reported to the Designated Safeguarding Leads.

- The authority to allow/block access to certain social sites (e.g. Twitter, Facebook) will remain with the Senior Leadership Team, in consultation with the Designated Safeguard Leads.

3.2.6 - Managing emerging technologies;

- Emerging technologies will be examined for educational benefit and consideration to suitability will be carried out before use in college is allowed.

- Mobile phones will not be used during lessons or formal college time. The sending of abusive or inappropriate text messages is forbidden.

3.2.7 - Protecting personal data;

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and General Data Protection Regulations (GDPR) 2018.

3.3 - Policy Decisions

3.3.1 - Assessing risks;

- The College will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a college computer. The College cannot accept liability for the material accessed, or any consequences of internet access.

- The College will take all reasonable measures to reduce access to inappropriate material and websites and will review safety protocols regularly.

3.3.2 - Handling e-safety complaints;

- Complaints of internet misuse will be dealt with by the Centre Manager, or a member of the Senior Leadership Team.

- Any complaint about staff misuse must be referred to the Centre Manager.

- Complaints of a child protection nature must be dealt with in accordance with SupaJam's Safeguarding Policy.

- Students and parents will be informed of the complaint's procedure.

- Discussions will be held with the Police Youth Crime Reduction Officer (or similar) to establish procedures for handling potentially illegal issues.

4. E-Safety Rules

4.1 - These e-Safety Rules help to protect students and The College by describing acceptable and unacceptable computer use.

- The College owns the computer network and can set rules for its use.

- It is a criminal offence to use a computer or network for a purpose not permitted by the college.

- Irresponsible use may result in the loss of network or internet access.

- Network access must be made via the user's authorised account and password, which must not be given to any other person.

- All network and internet use must be appropriate to education.

- Copyright and intellectual property rights must be respected.

- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.

- Anonymous messages and chain letters are not permitted.

- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.

- The College ICT systems may not be used for private purposes, unless the Senior Leadership Team has given specific permission.

- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The College may exercise its right to monitor the use of the computer systems, including access to web-sites, the deletion of inappropriate materials where it believes unauthorised use of The College's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

E-safety and Acceptable ICT Use Agreement

At SupaJam Education in Music and Media we are a technology rich environment and have invested considerable funds in providing students with the best equipment possible.

In order for this equipment to function to its full capacity it needs to be treated with respect.

We have an acceptable ICT use policy. These rules are to protect students and their work. We will take it very seriously if these guidelines are broken.

We take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a college computer. Neither The College nor Kent County Council can accept liability for the material accessed, or any consequences of internet access.

σ I have read the rules and I agree to abide by them:

Signature of Student...

Print... Date....................

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult The College's e‐safety policy for further information and clarification.

- The information systems are college property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that college information systems may not be used for private purposes, without specific permission from Senior Leaders.

- I understand that The College may monitor my information systems and internet use to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate manager.

- All internet activity should be appropriate. Appropriate means that the material accessed is not pornographic, obscene, racist, and offensive to any individual or legally questionable.

- All emails sent must not contain any material that is not appropriate (see above definition).

- All staff are responsible for the email they choose to open or store in their inbox – sensible decisions must be made on whom your email address is given to.

- I will not install any software or hardware without permission.

- I will ensure that personal data is kept secure and is used appropriately, whether in college, taken off The College premises or accessed remotely.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the Safeguarding Lead.

- I will ensure that any electronic communications with students are compatible with my professional role.

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

- I agree to look after any computer equipment issued to my care. I understand that if it is damaged and a claim is made on The College insurance policy, the following applies –

  i. If damage is due to my negligence, I will pay the excess

  ii. If damage is due to an accident, The College will pay the excess

iii. If the damage is due to wear and tear, The College will pay the excess

The decision on this will be made by the Centre Manager or Director of Programmes.

The College may exercise its right to monitor the use of The College's information systems, including internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of The College's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: .... Print: .... Date: ....

Accepted for college: .... Print: ....