# Online Safety Policy

**Purpose**

Online Safety encompasses the use of new technologies, internet and electronic communications such as learning platforms, mobile phones, tablets, video conferencing, collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

- This policy has links to other policies *e.g.* acceptable use, bullying, and child protection.
- There is a separate designated Child Protection Coordinator (see child protection policy).

**What are the risks?**

| | **Content**<br>Student as receiver (of mass productions) | **Contact**<br>Student as participant (adult-initiated activity) | **Conduct**<br>Student as actor (perpetrator / victim) |
|---|---|---|---|
| **Aggressive** | Violent / gory content | Harassment, stalking | Bullying, hostile peer activity |
| **Sexual** | Pornographic content | 'Grooming', sexual abuse on meeting strangers | Sexual harassment, 'sexting' |
| **Values**<br>The Academy acknowledges its responsibility to foster informed discussion and protect students from the potential harm caused by extremist* attitudes of all sorts.<br><br>**The Government has defined extremism in the Prevent Strategy 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."* | | | |
| | Racist, biased information / advice | Ideological persuasion | Potentially harmful user-generated content. Providing advice e.g. suicide / pro-anorexia |
| **Commercial** | Embedded marketing | Personal data misuse | Gambling, copyright infringement |

Adapted from Livingstone, S, and Haddon, L (2009) (re-examined in 2013) EU Kids Online: Final report. LSE, London: EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5)

**Requirements on Users**

- All staff, students and parents must read and sign the acceptable use contract (AUC) before using any of the Academy's ICT resource.
- The Academy has a central record of all staff and students who are granted ICT access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.
- Students are not permitted under the AUC to use ICT equipment unsupervised.
- Staff and students may only use the academy's e-mail accounts on the academy's system.
- Mobile phones must not be seen during formal academy time except under the direction of a teacher. The sending of abusive or inappropriate text messages is forbidden. Use of other personal devices for sound or image recording during formal academy time is also prohibited, except under the direction of a teacher.
- Staff will not use personal equipment or non-Academy personal electronic accounts when contacting students but will use their Academy email account or, where telephone contact is required, will be issued with an Academy phone.

**Features of the Academy System**

- Internet access is designed expressly for students and community use and includes filtering both at LA level and within the Academy appropriate to the age of the students.
- The Academy ensures through the AUC that the use of internet derived materials by staff and students complies with copyright law.
- The Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to *guarantee* that unsuitable material will *never* appear on an Academy computer. Neither the Academy nor the LA can accept liability for the material accessed, or any consequences of internet access.
- The Academy will block/filter access to social networking sites, newsgroups and external email systems. Circumventing this, *e.g.* via proxy servers, is forbidden under the AUC and will result in disciplinary action being taken.
- The Academy regularly audits ICT provision (in particular remote access logs and website tracking logs).
- Academy ICT systems are reviewed regularly for capacity and security including virus protection.
- Emerging technologies are examined for educational benefit and a risk assessment highlighting any necessary changes to this policy will be carried out before use in the Academy is allowed.

**Keeping Users Informed**

- Students are taught about what internet use is acceptable and given clear objectives for internet use in both Creative Computing and Media and EFL classes.
- Online safety rules are posted in all rooms where computers may be used and discussed with the students at the start of each year.
- All users are aware via the AUC that internet use is monitored and can be traced to the individual user.
- All staff have access to this Online Safety Policy and its importance will be explained to new staff members.
- Parents' attention will be drawn to the academy's Online Safety Policy when their children join the academy and again as appropriate *e.g.* in newsletters, the academy web site etc...

**Privacy**

- Students must not reveal personal details of themselves or others which may reveal their identity or location in any electronic communication, or arrange to meet anyone without specific permission. They are advised to this effect when signing the AUC as well as in relevant lessons.
- The only contact details on the Academy web site will be the Academy address, e-mail and telephone number. Staff or students' personal information will not be published.
- The Principal takes overall editorial responsibility for the website and ensures that content is accurate and appropriate.
- Parents and carers' consent for the publication of photographs of students and their work is obtained on joining the Academy and photographs of those who opt out are not used.
- Students must not access or copy images used for learning within lessons at any other times.
- Students' full names will not be used anywhere on any Academy system which is accessible to the public *e.g.* website, particularly in association with photographs.
- The AUC insists that computers be locked when not in use to help prevent unauthorised access to personal data; the lock activates automatically after a set time.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff who choose to access personal data *e.g.* student records from home, or remove such data from site on a removable storage device do so in the knowledge that they are bound by this act and must use an encrypted device.

**If something goes wrong …**

- Students must immediately tell a teacher if they receive an offensive electronic communication including e-mail or text messages.
- If students discover an unsuitable site it must be reported to a teacher and then via the support logging system to the IT Technician who will block/filter the site or escalate as appropriate.
- Complaints of internet misuse will be passed from the class teacher, or IT Technician to the Vice Principal with responsibility for whole-school strategic ICT.
- Complaints about staff misuse will be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with the Academy's child protection procedures.
- If any student should approach a member of staff with an allegation involving inappropriate text messages or images of a sexual nature it is not appropriate for that member of staff to attempt to verify the nature of these texts or images by asking to look at them or agreeing to do so if a student or other party offers to show them. The correct response is to pursue the matter promptly with one of our Designated Safeguarding Professionals (MK, GA, MY, SdP, DB). Those members of staff will seek police advice.

Approved at Student Progress & Achievement Committee: 13th November 2018
Review: Autumn Term 2019

This document is part of the group which include Safeguarding, Child Protection, Behaviour for Learning, Anti-Bullying, Acceptable Use, Exclusions, Policy Statement Additional & Special Education Needs, Drugs' Education, Use of Images, Student Illness, Accident & First Aid, Use of Force, Recruitment, Supporting Children with Medical Conditions, Single Equality Scheme and Health & Safety Policies.

This document is also part of the group which include Freedom of Information, Safekeeping of Loaned ICT/AV Equipment and Information Risk Management Policies.