Sidney Stringer
Multi Academy Trust

E-Safety Policy

September 2016 – September 2018

Sidney Stringer
Multi Academy Trust

INTRODUCTION

It is the duty of the Multi Academy Trust to ensure that children and young people are protected from potential harm both within and beyond the Academy environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

The Trust will ensure that the following are in place in relation to E-safety:

- Firewalls
- Anti-virus and anti-spyware software
- Filters
- Using an accredited ISP (internet Service Provider)
- Awareness of wireless technology issues
- A clear policy on using personal devices

1. INTERNET

The internet is an essential element in 21st century life for education, business and social interaction. The Multi Academy Trust 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. The MAT Internet access will be designed expressly for student use and will include filtering which is provided either by the Local Authority or through bespoke filtering using Lightspeed bottle rocket (as is the case at SSA).

Students will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.

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

The Trust will ensure that staff and students are educated and aware of the limitations of internet derived materials and the need to comply with copyright laws.

2. MANAGING INTERNET ACCESS

The MAT ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed and reviewed with the MAT ICT Network team.

2.1 Email

- Students will have access to an email address.
- Students must immediately inform a teacher if they receive offensive emails.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone.
- Email sent to an external organisation should be written carefully in line with other external Academy communication.
- The forwarding of chain letters is not permitted.

2.2 Published content and the websites

- The websites should include details of each Academy location and contact number. Email addresses will be published for certain staff.
- The Principal/headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3 Publishing students' images and work

Students' images will be published where permission has been given. Students' work may also be published on the web.

2.4 Social networking and Social media

Academies/Schools will filter social media sites and students will not be authorised to use these sites on Academy equipment.

Students and parents will be advised on the safe use of social media/network spaces outside the Academy.

In addition to this the following applies to staff at the Academy when using these sites:

- All comments must be in support of the Academy and Academy policy
- Any confidential policy items or issues must not be disclosed
- Any personal events or issues should only be posted if you would be happy speaking these publically to parents or students.
- You should not be friends with any student or former student if under 18 on facebook/social networking or media sites or if they are still connected to the Academy/school via siblings or relatives, and should lock down your profile to ensure they cannot get access by accident (see details below).
- You should not add images of any students at the Academy/school without permission from the Principal/headteacher
- You should not add images of the Academy/School that may be deemed inappropriate.

2.5 Managing filtering

The Multi Academy Trust will work with the Internet Service Provider, ICov and the MAT Network team to ensure systems to protect students are reviewed and improved.

If staff or students discover an unsuitable site it must be reported to the MAT Network Team's Help Desk.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.6 Managing emerging technology and video conferencing

Video conferencing will be supervised and will go through the Academy/school internet. Emerging technology will be examined for educational benefit and risks will be assessed before use in the Academy/school is allowed.

Mobile phones and mobile technology such as iPads is permitted for students but the following rules will apply:

1. Mobile devices can only be used in lessons if the teacher has given prior permission
2. If a device is misused in lessons (misuse constitutes not using the mobile device for the task assigned, e.g. social media sites, videos, games etc.), then the teacher can confiscate the mobile device until the end of the lesson.
3. If the misuse is deemed serious then the mobile device will be confiscated until the end of the day and given to the students House Head or Lead member of staff in charge of New Technology.
4. If there is an incident which is severe then the mobile device will be confiscated and not returned until parents have been met with. In some cases if illegal software or videos are downloaded students will be reported to the relevant authorities.

Students will be responsible for their own devices at all times and need to ensure that they are kept safe and secure. The Academy/school will not be responsible for student equipment.

2.7 Protecting Personal Data

Personal data will be recorded, transferred and made available according to the Data Protection Act 1988.

3. POLICY DECISIONS

3.1 Authorising ICT access and Internet Access

All students and staff must read and sign the, “Acceptable Use Agreement” before using any Academy/school ICT resource.

The Academy/school will keep a record of all staff and students who have access. The Academy/school have the right to withdraw ICT access form both staff and students.

3.2 Assessing risks

The Academy/school 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 or device. Neither the Multi Academy Trust or ICov can accept liability for material accessed or any consequence of internet access.

The Academy/school will audit ICT provision to ensure the e-safety policy is adequate and that its implementation is effective.

3.3 Handling E- safety complaints

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher/Principal. Complaints of a child protection nature must be dealt with in accordance with Multi Academy Trust child protection procedures.

Students and parents will be informed of the complaints procedure.

3.4 External providers and community use of the ICT facilities and internet

The Academy/school will authorise any use required by the community or external providers. All groups must adhere to the e- safety policy and sign the ICT acceptable use policy.

4. COMMUNICATION OF THE E-SAFETY POLICY

E- safety will be discussed with students each academic year as part of either the tutorial programme or ICT lessons.

Students will be informed that the network and internet use will be monitored.

All staff will have access to the E-safety policy via the Academy/school website and its importance reiterated via email communication or other means.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretions and professional conduct is essential.

4.1 Enlisting parents' support

Parents' attention will be drawn to the Academy/school E-safety policy though the Academy website and Parent Council meetings.

5. TEACHING AND LEARNING

Teachers are encouraged to use ICT for both teaching and learning and also to add interest and to motivate students. This must always be done within the limits of the E-safety policy.