Mulberry
Academy Shoreditch

E-Safety Policy

Recommending Body:	MAS LGB
Approval Body:	MAS LGB
Approval Date:	November 2019
Implementation Date:	November 2019
Review Date:	November 2020
Status:	Approved
Policy Version:	1

Introduction

1.1 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.

1.2 The academy's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Anti-Bullying, Safeguarding and Data Protection.

1. END TO END E-SAFETY

2.1 E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies and taught lessons covering e-safety.
- Sound implementation of the e-safety policy in both administration and curriculum, including secure academy network design and use.
- The supply of a safe and secure broadband connection from London Grid for Learning (LGfL), via the approved broadband supplier.
- The use of LGfL to monitor and filter student activity on the internet.

2. E-SAFETY POLICY AT MULBERRY ACADEMY SHOREDITCH

3.1 Our e-safety policy has been agreed by senior management and approved by the Local Advisory Body. The e-safety policy and its implementation will be reviewed annually.

3. TEACHING AND LEARNING

3.1 Why Internet Use is Important

- The internet is an essential element in 21st century life for education, business and social interaction. The academy 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.

3.2 Internet Use will Enhance Learning

- The academy's internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- 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 internet in research, including the skills of knowledge location, retrieval and evaluation.

3.3 Students will be Taught How to Evaluate Internet Content

- Schools should ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4. MANAGING INTERNET ACCESS

4.1 Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection provided by LGfL will be installed and updated regularly.
- The results of misuse collected by Impero monitoring software will be reviewed and the necessary steps be taken with those breaking rules.

4.2 Email

- All students and staff have a network account and individual email address.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully in the way as a letter written on academy headed paper.
- The forwarding of chain letters is not permitted.

4.3 Published Content and the Academy Website

- The contact details on the website should be the academy address, emails and telephone number. Staff or students personal information will not be published although pictures of students may be accessible.

- The Principal supported by a member of the senior leadership team with responsibility for ICT will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.4 Publishing Student Images and Work

- Photographs that include students will be selected carefully.
- Written notice will be given to all parents on an annual basis with regard to photographs of students being published on the academy website and other academy publications.
- Students work can only be published with the permission of the student.

4.5 Social Networking and Personal Publishing

- The school will block/filter access to social networking sites (eg. Facebook, Instagram and chatrooms).
- Newsgroups will be blocked unless a specific use is approved.
- Students will be given advice on how to limit the risks of social media use outside school, and in particular:
    - Students will be advised never to give out personal details of any kind which may identify them or their location.
    - Students will be advised not to place personal photos on any social networking space.
    - 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.

5.6 Managing Filtering

- The school will work in partnership with LGfL in monitoring all content when accessing the internet or other ICT related tasks. In addition, the academy has Impero software that monitors and alerts the ICT department and Safeguarding Designated Person of any searches for key words deemed inappropriate by the academy.
- If staff or students discover an unsuitable site, it must be reported to the ICT Co-ordinator.
- ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

5.7 Managing Video Conferencing

- Video conferencing will be appropriately supervised for all students.

5.8 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and risk assessed before use in the academy is allowed.
- Mobile phones will be switched off throughout the school day (whilst a student is on the academy's premises).
- Wireless network will not be available to students for mobile use.
- The use of mobile technology to send abusive or inappropriate text messages or email is forbidden as is the videoing or photographing of others without permission.

5.9 Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

5. POLICY DECISIONS

5.1 Authorising Internet Access

- All staff and students must read and agree to the Acceptable Use Policy before using any school ICT resource.
- The school will maintain a current record of all staff and students who are granted access to academy ICT systems.
- Access to the ICT resources and or the internet will be withdrawn should the system be used inappropriately. This will be in addition to any sanction applied under the academy's Behaviour Policy (in respect of students) or Disciplinary Policy (in respect of staff).

6.1 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material, and material which could expose students to harm. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will not appear on an academy computer. Neither the academy nor the ICT coordinator can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

5.2 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 Principal.
- Complaints of a child protection nature must be dealt with in accordance with academy child protection procedures, which can be found in the Safeguarding Policy.

6. COMMUNICATIONS POLICY

6.1 Introducing the E-Safety Policy to Students

- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and internet use will be monitored.

6.2 Staff and the E-Safety Policy

- This e-safety policy will be referred to within the teachers' handbook and presented to all new staff; it will be stored on the intranet with access for all staff.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

6.3 Enlisting Parents' Support

- Parent's attention will be drawn to the school E-safety Policy in newsletters and via other appropriate events.