FUTURE ACADEMIES – E-SAFETY Policy

Document control table			
Document title:		E-Safety Policy	
Author (name & job title):		Shanaaz Price Governance and Compliance Officer	
Version number:		V1	
Date created:		04.10.17	
Date approved:		06.10.17	
Approved by:		Governing Body	
Review information:		This document is reviewed internally annually, and is reviewed by the Board of Directors every two years.	
Last internal review:		October 2017	
Last review by Governors/Directors:		October 2017	
Document History			
Version	**Date**	**Author**	**Note of revisions**
V1	04.10.17	SP	

CONTENTS

1. SCOPE

1. This e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and child protection.

2. The policy applies to the Headteacher and to all staff employed by the Academy.

2. PURPOSE

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

    a. The e-Safety Policy and its implementation will be reviewed annually.

    b. Our e-Safety Policy has been written by the Academy, building on the LBHF e–Safety Policy and government guidance and has been discussed with Staff and by the School Council.

    c. Our Academy Policy has been agreed by the Senior Leadership Team and reviewed by Trustees.

    d. Training for staff and students will take place to ensure full understanding and compliance with the policy.

3. TEACHING AND LEARNING

1. Internet use is important

    a. Internet use is part of the statutory curriculum and is a necessary tool for learning.

    b. The Internet is a part of everyday 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.

    c. Students use the Internet widely outside of the Academy and need to learn how to evaluate Internet information and to take care of their own safety and security.

    d. The purpose of Internet use in the Academy is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management functions.

2. Internet use enhances learning

    a. The Academy's Internet access will be designed to enhance and extend education.

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

    c. The Academy will ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law.

    d. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.

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

3. Students will learn how to evaluate Internet content

    a. Students will use age-appropriate tools to research Internet content.

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

    c. Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

    d. Students will be taught how to report unpleasant Internet content eg using the CEOP Report Abuse icon.

4. MONITORING E-SAFETY

1. Maintaining information systems security

    a. The security of the Academy information systems and users will be reviewed regularly.

    b. Virus protection will be updated regularly.

    c. Personal data sent over the Internet or taken off site will be encrypted.

    d. Portable media may not be used without specific permission followed by an anti-virus / malware scan.

    e. Unapproved software will not be allowed in work areas or attached to email.

    f. Files held on the Academy's network will be regularly checked.

    g. The ICT department will review system capacity regularly.

    h. The use of user logins and passwords to access the Academy network will be enforced.

2. Managing email

    a. Students may only use approved email accounts for Academy purposes.

    b. Students must immediately tell a designated member of staff if they receive offensive email.

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

    d. Staff will only use official Academy provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team.

    e. Excessive social email use can interfere with learning and will be restricted.

    f. Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper would be.

    g. The forwarding of chain messages is not permitted.

    h. Staff should not use personal email accounts for Academy purposes.

3. Managing published content

    a. The contact details on the website should be the Academy address, email and telephone number. Staff or students' personal information must not be published.

    b. Email addresses will be published carefully online, to avoid being harvested for spam (eg by replacing '@' with 'AT'.)

    c. The Headteacher will take overall editorial responsibility for online content published by the Academy and will ensure that content published is accurate and appropriate.

    d. The Academy website will comply with the Academy's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

4. Publishing students' images or work

    a. Images or videos that include students will be selected carefully and will not provide material that could be reused.

    b. Students' full names will not be used anywhere on the website, particularly in association with photographs.

    c. Written permission from parents or carers will be obtained before images/videos of students are electronically published.

    d. Students' work can only be published with permission from the student or the parents.

e. Written consent will be kept by the Academy where students' images are used for publicity purposes, until the image is no longer in use.

f. The Academy will have a policy regarding the use of photographic images of children which outlines policies and procedures.

5. Managing social networking, social media and personal publishing

a. The Academy will control access to social media and social networking sites.

b. Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, Academy attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

c. Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using social media tools in the classroom.

d. Staff official blogs or wikis should be password protected and run from the Academy website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for student use on a personal basis.

e. Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the Academy where possible.

f. Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

g. All members of the Academy community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

h. Newsgroups will be blocked unless a specific use is approved.

i. Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of Academy) will be raised with their parents/carers, particularly when concerning underage students' use of sites.

j. Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Academy Acceptable Use Policy.

6. Managing filtering

    a. The Academy's broadband access will include filtering appropriate to the age and maturity of students.

    b. The Academy will work with LBHF and the Academy's ICT department to ensure that filtering policy is continually reviewed.

    c. The Academy will have a clear procedure for reporting breaches of filtering. All members of the Academy community (all staff and all students) will be aware of this procedure.

    d. If staff or students discover unsuitable sites, the URL will be reported to the Academy ICT department who will then record the incident and escalate the concern as appropriate.

    e. The Academy filtering system will block all sites on the Internet Watch Foundation (IWF) list.

    f. Changes to the Academy filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and, where appropriate, with consent from the Senior Leadership Team.

    g. The Academy Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

    h. Any material that the Academy believes is illegal will be reported to appropriate agencies such as IWF, Hammersmith Police or CEOP

    i. The Academy's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from the ICT department.

7. Managing video communication

    a. All video communication equipment in the classroom must be switched off when not in use and not set to auto answer.

    b. External IP addresses will not be made available to other sites.

    c. Video communication contact information will not be put on the Academy Website.

    d. The equipment must be secure and if necessary locked away when not in use.

    e. Academy video communication equipment will not be taken off Academy premises without permission.

    f. Responsibility for the use of the video communication equipment outside Academy time will be established with care.

    Users

    g. Students will ask permission from a teacher before making or answering a video communication.

h. Video communication will be supervised appropriately for the students' age and ability.

i. Parents and carers consent should be obtained prior to children taking part in video communications.

j. Only key administrators should be given access to video communication administration areas or remote control pages.

k. Unique log on and password details for the educational video communication services should only be issued to members of staff and kept secure.

8. Managing emerging technologies

a. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.

b. Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Academy Acceptable Use or Mobile Phone Policy.

9. Protecting personal data

a. Personal data will be recorded, processed, transferred and made available according to the GDPR Dat Protection Act 1998/2018.

5. POLICY DECISIONS

1. Authorising Internet access

b. The Academy will maintain a current record of all staff and students who are granted access to the Academy's network.

c. All new staff will read and sign the 'Academy Acceptable Use Policy' before using any Academy ICT resources. Existing staff are reminded of the requirement to adhere to all Academy Policies.

d. When considering access for vulnerable members of the Academy community (such as with children with special education needs) the Academy will make decisions based on the specific needs and understanding of the student(s).

e. Secondary students will apply for Internet access individually by agreeing to comply with the 'Academy e-Safety Rules' and 'Acceptable Use Policy'.

2. Risk assessment

a. The Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global, changing and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via an Academy computer. Neither the Academy nor LBHF can accept liability for the material accessed, or any consequences resulting from Internet use.

b. The Academy will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

c. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990/1998 and breaches will be reported to Hammersmith Police.

d. Methods to identify, assess and minimise risks will be reviewed regularly.

3. Responding to any incidents of concern

a. All members of the Academy community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).

b. The ICT department will record all reported incidents and actions taken in the Academy e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

c. The ICT department will inform the Designated Child Protection Coordinator of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

d. The Academy will manage e-Safety incidents in accordance with the Academy discipline/ behavior policy where appropriate.

e. The Academy will inform parents/carers of any incidents of concerns as and when required.

f. After any investigations are completed, the Academy will debrief, identify lessons learnt and implement any changes required.

g. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Academy will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.

h. If the Academy is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.

i. If an incident of concern needs to be passed beyond the Academy then the concern will be escalated to the e-Safety officer to communicate to other Academies in Hammersmith and Fulham.

4. E-safety complaints

a. Complaints about Internet misuse will be dealt with under the Academy's complaints procedure.

b. Any complaint about staff misuse will be referred to the Head Teacher.

c. All e-Safety complaints and incidents will be recorded by the Academy, including any actions taken.

d. Students and parents will be informed of the complaints procedure.

e. Parents and students will need to work in partnership with the Academy to resolve issues.

f. All members of the Academy community will need to be aware of the importance of confidentiality and the need to follow the official Academy procedures for reporting concerns.

g. Discussions will be held with the local Police Safer Academy's Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.

h. Any issues (including sanctions) will be dealt with according to the Academy's disciplinary, behaviour and child protection procedures.

i. All members of the Academy community will be reminded about safe and appropriate behavior online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Academy community.

5. Internet use across the community

a. The Academy will liaise with local organisations to establish a common approach to e-Safety.

b. The Academy will be sensitive to Internet-related issues experienced by students out of Academy, e.g. social networking sites, and offer appropriate advice.

c. The Academy will provide appropriate levels of supervision for students who use the internet and technology whilst on the Academy site.

d. The Academy will provide an Acceptable Use Policy for any guest who needs to access the Academy computer system or internet on site.

6. CYBERBULLYING

1. How will Cyberbullying be managed?

a. Cyberbullying (along with all other forms of bullying) of any member of the Academy community will not be tolerated. Full details are set out in the Academy's policy on anti-bullying and behaviour.

b. There are clear procedures in place to support anyone in the Academy community affected by cyberbullying.

c. All incidents of cyberbullying reported to the Academy will be recorded.

d. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

e. Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

f. The Academy will take steps to identify the bully, where possible and appropriate. This may include examining Academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

g. Students, staff and parents/carers will be required to work with the Academy to support the approach to cyberbullying and the Academy's e-Safety ethos.

h. Sanctions for those involved in cyberbullying may include:
   - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
   - Internet access may be suspended at the Academy for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the Academy's anti-bullying, behaviour policy or Acceptable Use Policy.
   - Parent/carers of students will be informed.
   - The Police will be contacted if a criminal offence is suspected.

7. MANAGING LEARNING PLATFORMS

1. SLT and staff will regularly monitor the usage of the Learning Platform (LP) by students and staff in all areas, in particular message and communication tools and publishing facilities.

2. Students/staff will be advised about acceptable conduct and use when using the LP.

3. Only members of the current student, parent/carers and staff community will have access to the LP.

4. All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

5. When staff, students etc leave the Academy their account or rights to specific Academy areas will be disabled or transferred to their new establishment.

6. Any concerns about content on the LP may be recorded and dealt with in the following ways:

   a. The user will be asked to remove any material deemed to be inappropriate or offensive.

   b. The material will be removed by the site administrator if the user does not comply.

   c. Access to the LP for the user may be suspended.

   d. The user will need to discuss the issues with a member of SLT before reinstatement.

   e. A student's parent/carer may be informed.

7. A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
8. Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

8. MOBILE PHONES AND PERSONAL DEVICES

1. Use of Mobile Phones

    a. The use of mobile phones and other personal devices by students and staff in Academy will be decided by the Academy and covered in the Academy Acceptable Use Policy

    b. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Academy community and any breaches will be dealt with as part of the Academy discipline/behaviour policy.

    c. Academy staff may confiscate a phone or device if they believe it is being used to contravene the Academy's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the student or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

    d. The use of personal devices as network hot-spots is strictly forbidden.

    e. Electronic devices of all kinds that are brought in to Academy are the responsibility of the user. The Academy accepts no responsibility for the loss, theft or damage of such items. Nor will the Academy accept responsibility for any adverse health effects caused by any such devices, either potential or actual.

2. Students' Use of Personal Devices

    a. Mobile phones should be switched off and at the bottom of the student's bag at all times. If a student breaches the Academy policy then the phone or device will be confiscated and will be held in a secure place in accordance with the Academy policy.

    b. Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

    c. If a student needs to contact his/her parents/carers they will be allowed to use an Academy phone. Parents are advised not to contact their child via their mobile phone during the Academy day, but to contact the Academy office. Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed on safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

3. Staff Use of Personal Devices

    a. Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

    b. Staff will be issued with an Academy phone where contact with students or parents/carers is required.

    c. Mobile Phones and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

    d. If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

    e. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose

    f. If a member of staff breaches the Academy policy then disciplinary action may be taken.

9. COMMUNICATION POLICY

1. How will the policy be introduced to students?

    a. All users will be informed that network and Internet use will be monitored.

    b. Student instruction regarding responsible and safe use will precede Internet access.

    c. An e-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe Academy and home use.

    d. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

    e. Particular attention to e-Safety education will be given where students are considered to be vulnerable.

2. How will the policy be discussed with staff?

    a. To protect all staff and students, the Academy will implement Acceptable Use Policies.

    b. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

    c. Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

d. Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

e. The Academy will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.

f. All members of staff will be made aware that their online conduct out of Academy could have an impact on their role and reputation within Academy. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

3. How will parents' support be enlisted?

a. Parents' attention will be drawn to the Academy e-Safety Policy in newsletters, the Academy prospectus and on the Academy website.

b. A partnership approach to e-Safety at home and at Academy with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events eg parent evenings and sports days.

c. Parents will be encouraged to read the Academy Acceptable Use Policy for students and discuss its implications with their children.

d. Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.

e. Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.