BRIDGE ACADEMY

The Bridge Academy
Laburnum Street, Hackney, London E2 8BA
Tel: 020 7749 5240
Principal: Mr C Brown

E-Safety Policy

Author: **Principal**

Reviewed: **Annually**

Approved: June 2018

Review Date: June 2019

Background

New technologies have become integral to the lives of children and young people in today's society, and their use has been shown to raise educational standards and promote student achievement.

The internet and other digital and information technologies are powerful tools which can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. The Academy will do everything in its power to support this. However, the use of these new technologies can put young people at risk within and outside the Academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being groomed by those with whom they make contact on the internet
- The sharing / distribution of personal images without consent and / or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- Additional problems caused by an inability to evaluate the quality, accuracy and relevance of information on the internet.

Aims and Purpose

The aim of The Bridge Academy E-Safety Policy is to:

- Ensure the safe and appropriate use of technology by all relevant parties.
- Mitigate the above risks through good education provision so that students have the knowledge, confidence and skills to face and deal with these risks in the best manner possible.
- Address wider educational issues in order to help young people (and their Parents/Carers) to be responsible and safe users of the internet and other communication technologies, whether this is for educational, personal or recreational use.

It should be noted that many of these risks reflect situations in the off-line world, and so this E-Safety Policy must be used in conjunction with other Academy policies. A list of associated policies can be found at the end of this document.

Scope of the Policy

This Policy applies to all members of the Academy community (including staff, volunteers, Parents / Carers, visitors, community users) who have access to and / or are users of Academy ICT systems, both in and outside the Academy.

The Education and Inspection Act 2006 empowers the Principal to such extent as is reasonable, to regulate the behaviour of students when they are off the Academy site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of Cyber-bullying, or other E-Safety incidents covered by this Policy, which may take place out of the Academy but are linked to memberships of the Academy.

The Academy will deal with such incidents within this Policy and associated Behaviour for Learning and Anti-bullying Policies and will, where possible, inform Parents / Carers of incidents of inappropriate E-Safety behaviour that takes place out of the Academy.

Development / Monitoring / Review of this Policy

The E-Safety Policy has been developed by the Academy Principal, in consultation with the Academy Inclusion Manager and Safeguarding Lead, the Head of IT, the E-Safety Coordinator, the Senior Leadership Team and the Governing Body.

- The implementation of this E-Safety Policy will be monitored by: The Principal and Senior Leadership Team, Head of IT and E-Safety Coordinator
- Monitoring will take place at regular intervals: At agreed and relevant times during the Academy year.
- The Governing Body will receive a report on the implementation of the E-Safety Policy generated by the monitoring group at regular interviews: At agreed and relevant times during the Academy year.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to E-Safety or incidents that have taken place.

The Academy will monitor the impact of the Policy using:

- Logs of reported incidents
- Internal monitoring of data for network activity
- Surveys/questionnaires from:
    - Students (e.g. Ofsted “Tell-us” survey/CEOP Think Know Survey)
    - Parents/Carers
    - Staff.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the Academy:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy. This will be carried out by them receiving regular information about E-Safety incidents and monitoring reports. It is suggested that a member of the Governing Body will take on the role of E-Safety Governor. The role of E-Safety Governor will include:

- Regular feedback from the E-Safety / Computing Coordinator, Principal and technicians.

Principal and Senior Leaders:
The Principal is responsible for ensuring the safety (including E-Safety) of members of the Academy community, though day to day responsibility for E-Safety will be delegated to the Head of IT and E-Safety Coordinator.

The Principal and other members of the Senior Leadership Team will:

- Take the lead in establishing and reviewing the Academy E-Safety Policies/documents
- Ensure that the Head of IT and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as appropriate
- Ensure that there is a system in place to allow for monitoring and support of those in the Academy who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- Be responsible for implementing the appropriate procedure in the event of a serious E-Safety allegation being made against a member of The Bridge Academy
- Ensure that all staff members are aware of the procedures that need to be followed in the event of an E-Safety incident.

The Senior Leadership Team will receive regular monitoring reports from the Head of IT.

E-Safety Coordinator:
The E-Safety Coordinator is responsible for:

- Reporting regularly to the SLT
- Ensuring that the appropriate signage is in place
- Ensuring that E-Safety displays are kept up to date
- Designing and completing regular audits of the E-Safety needs of staff
- Providing training and advice for teaching staff.

Head of IT:
It is the role of the IT Manager to:

- Take day to day responsibilities for E-Safety issues
- Receive reports of E-Safety incidents and create a log of incidents to inform Future-Safety developments
- Report regularly to the E-Safety Coordinator and Principal.

Technical Staff:
The Academy technicians are responsible for ensuring that:

- The Academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- The Academy meets the E-Safety technical requirements
- Users may only access the Academy's networks through a properly enforced Password Protection Policy, in which passwords are regularly changed

- They stay up-to-date with E-Safety technical information in order to effectively carry out their Safety role, and inform and update other as relevant
- The use of the network / email is regularly monitored in order that any misuse / attempted misuse can be promptly reported to the E-Safety Coordinator and Principal for investigation / action / sanction.

Teaching and Support Staff:
Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current Academy E-Safety Policy and practices
- They have read and understood the Academy Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the relevant party for investigation
- Digital communications with students (typically, but not limited to, email) are on a professional level and only carried out using official Academy systems
- E-Safety best practice is embedded in all aspects of the curriculum and other Academy activities
- Students understand and follow the Academy E-Safety and Acceptable Use Agreement
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor IT activity in lessons and during extra-curricular and extended Academy activities
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current Academy policies with regard to these devices
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Inclusion Manager (Designated Safeguarding Lead):
The Inclusion Manager monitors E-Safety issues and should be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying.

The Inclusion Manager is responsible for ensuring that the Safeguarding and Child Protection Policy is followed where appropriate as part of the Academy approach to E-Safety. See the Academy Safeguarding and Child Protection Policy for more details.

Students:

All students must:

- Sign the Student Acceptable Use Agreement before being given access to Academy systems, and follow this at all times
- Understand the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, and know how to do so
- Know and understand the Academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Academy policies on taking / use of images or cyber-bullying
- Understand the importance of adopting good E-Safety practice when using digital technologies outside the Academy, and know that the Academy's E-Safety Policy covers their actions outside the Academy where they are related to their membership of the Academy. See the Academy Behaviour for Learning and Anti-bullying policies for more detail.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be responsible for:

- Endorsing (by signature) and supporting the Student Acceptable Use Agreement.

Spiritual, Moral, Social and Cultural Development (SMSC) and Prevent Duty:

As of 1 July 2015, Academies now have a legal duty to prevent students becoming radicalised, which has implications for SMSC, E-Safety and the general use of technology in the Academy. This will be approached diligently – see the Academy Safeguarding and Child Protection Policy for more detail.

E-Safety Education for Parents/Carers:

Many Parents and Carers have only a limited understanding of E-Safety risks and issues. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide." (Byron Report). The Academy will therefore seek to provide information awareness to Parents and Carers through:

- Letters, the newsletter, the Academy website and E-Safety leaflets
- Parents' evening.

Education and Training – Staff:

It is essential that all staff receive E-Safety training and understand their responsibility, as outlined in this Policy. Training will be offered as follows:

- A planned programme of informal E-Safety training will be made available to staff. An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process

- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the Academy E-Safety updates as part of their safeguarding training
- The Head of IT and ICT / Computing Subject Leader will receive regular updates through attending training sessions and regularly reviewing guidance documents
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET Days.

Curriculum:

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use. Any unsuitable material that is found in internet searches must be referred to IT for blacklisting
- Where students are allowed to freely search the internet, for example when using search engines, staff must be vigilant in monitoring the content of the websites the young people visit
- It is acceptable that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Head of IT (or other relevant person) temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons provided.
- Students should be taught in all lessons to be critically aware of the materials / content they access-on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Additionally:

- Rules for use of the internet are clearly displayed in the IT Suite and located near computers in each classroom
- Staff should act as good role models in their use of IT, the internet and mobile devices
- Key E-Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.

Use of Digital / Video images, student work and students' names

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are also many reported incidences of employers carrying out internet searches for information about potential and existing employees.

The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential harm as follows:

- When using digital images, staff should inform and educate students about the risks associated with taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, for example on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images.
- Images of students must not be taken on personal equipment
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or Academy into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Student's full names will not be used anywhere on a website, or blog, particularly in association with photographs
- Written permission from Parents or Carers will be obtained before photographs of students are published on the Academy website
- Student's work can only be published with the permission of the student and Parents or Carers.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1988 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

Comply with the Academy's Data Protection Policy

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its use or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

- Transfer sensitive data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, where possible:

- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with Academy policy once it has been transferred or its use is complete.

Please see Data Protection Policy for further information.

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Academy currently considers the benefit of using these technologies for education outweighs their risk/disadvantages.

Staff and other adults					Students		
* Students are only permitted to have phones in the Academy if they are switched off and in a pocket. If a student's mobile is seen or heard in the Academy it will be confiscated.	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Not allowed
* Mobile phones	X				X		
Use of mobile phones in lessons				X			X
Use of mobile phones in social time		X					X
Use of TBA iPads	X				X		
Use of Academy email for personal emails				X			X
Use of chat rooms / facilities				X			X
Use of instant messaging				X			X
Use of social networking sites			X				X
Use of blogs	X				X		

Email Protocol:

- The official Academy email service may be regarded as safe and secure and is monitored. Staff should therefore use the Academy email service to communicate with others when in the Academy or on Academy systems (e.g. by remote access)
- Users must immediately report to the nominated person in accordance with the Academy's policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Staff must not respond to any such email
- Any digital communication between staff and students or Parents / Carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) Academy systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff

Unsuitable/Inappropriate Activities:

The Academy believes that the activities referred to in the following section would be inappropriate in an Academy context and that members of the Academy should not engage in these activities in the Academy or outside the Academy when using Academy equipment or systems. The Academy policy restricts certain internet usage as follows:

- Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:
    - Anything that could be deemed illegal
    - Pornography
    - Promotion of any kind of discrimination
    - Promotion of racial or religious hatred, or radicalisation
    - Threatening behaviour, including promotion of physical violence or mental harm
    - Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute

- The following user actions are unacceptable:
    - Using Academy systems to run a private business
    - Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguarding employed by The Bridge Academy
    - Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary permissions
    - Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer/network access codes and passwords)
    - Creating or propagating computer viruses or other harmful files

- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Any use contrary to the Academy's IT policies.

Illegal activity will be reported to the authorities including Police where appropriate. It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents will be dealt with as soon as possible in a proportionate manner through normal behaviour / disciplinary procedures as appropriate. The flowchart attached outlines the procedure to be followed following an E-Safety incident.

Staff may refer to the following websites for guidance and further information:

https://www.ceop.police.uk/

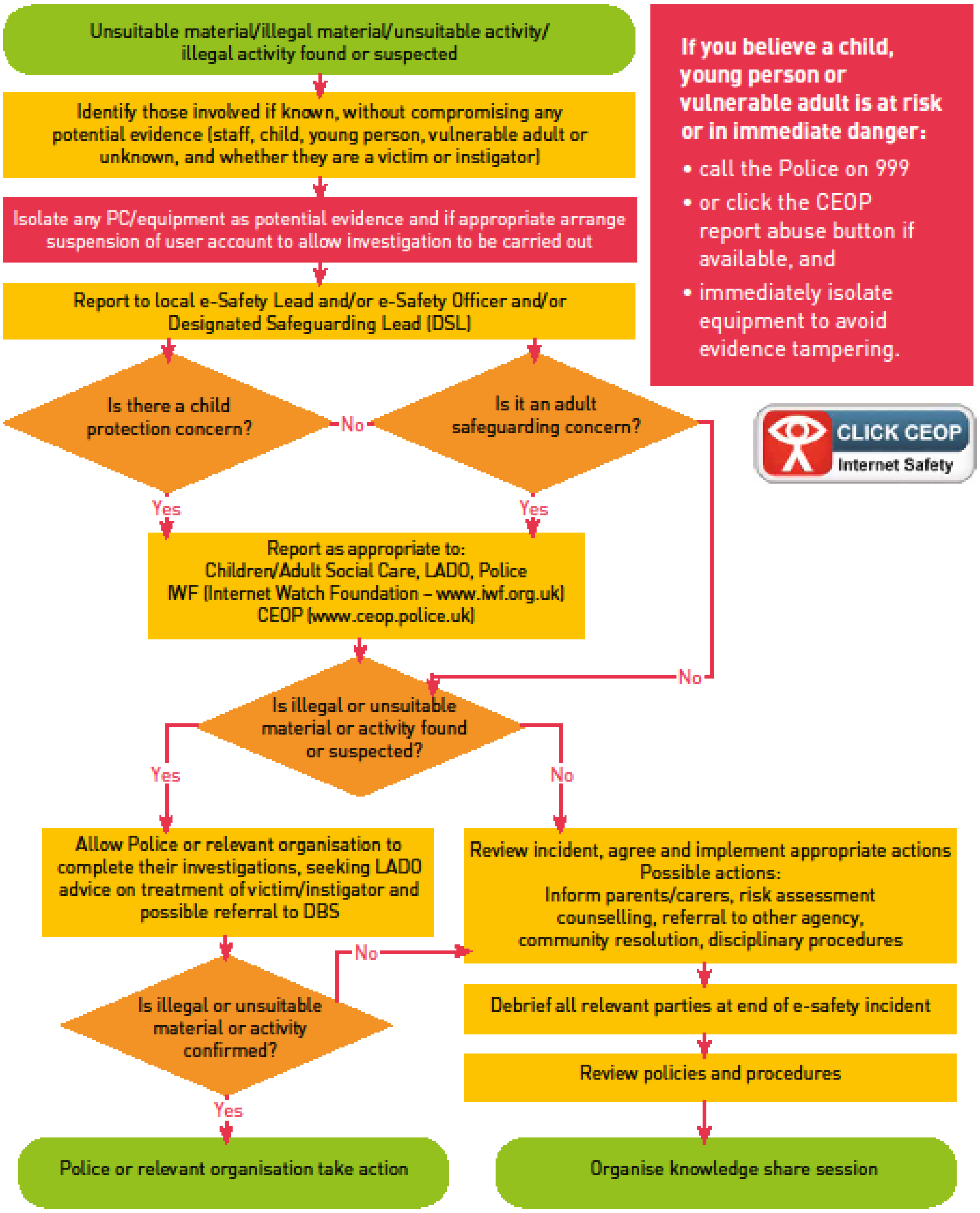
https://www.thinkuknow.co.uk

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Related Policies:

Safeguarding and Child Protection Policy
Data Protection Policy
Behaviour for Learning Policy
Social Media Policy
ICT Policies Combined
Acceptable Use Agreement

e-Safety Incident Flowchart



Unsuitable material/illegal material/unsuitable activity/ illegal activity found or suspected

Identify those involved if known, without compromising any potential evidence (staff, child, young person, vulnerable adult or unknown, and whether they are a victim or instigator)

Isolate any PC/equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out

Report to local e-Safety Lead and/or e-Safety Officer and/or Designated Safeguarding Lead (DSL)

Is there a child protection concern?

Is it an adult safeguarding concern?

Report as appropriate to:
Children/Adult Social Care, LADO, Police
IWF (Internet Watch Foundation – www.iwf.org.uk)
CEOP (www.ceop.police.uk)

Is illegal or unsuitable material or activity found or suspected?

Allow Police or relevant organisation to complete their investigations, seeking LADO advice on treatment of victim/instigator and possible referral to DBS

Review incident, agree and implement appropriate actions
Possible actions:
Inform parents/carers, risk assessment counselling, referral to other agency, community resolution, disciplinary procedures

Is illegal or unsuitable material or activity confirmed?

Debrief all relevant parties at end of e-safety incident

Review policies and procedures

Police or relevant organisation take action

Organise knowledge share session

If you believe a child, young person or vulnerable adult is at risk or in immediate danger:

- call the Police on 999
- or click the CEOP report abuse button if available, and
- immediately isolate equipment to avoid evidence tampering.

CLICK CEOP
Internet Safety