E-Safety Policy

RIVERSIDE BRIDGE SCHOOL

'EXCELLENCE FOR ALL'

London Borough of Barking & Dagenham

Ratified by Governors: March 2023

To be reviewed: September 2023

Riverside Bridge School

E-SAFETY POLICY

Review Frequency:	Annually
Date of ratification:	March 2023
Date next review due:	September 2023
Scope of Policy:	This policy applies to all staff, students, governors and volunteers at Riverside Bridge School

Headteacher:

Mrs K Cerri
kice@riverside.bardaglea.org.uk
Ext: 201060

Deputy Headteacher:

Ms L Amri
leam@riverside.bardaglea.org.uk
Ext: 201100

Assistant Headteacher:

Mrs H Clark
hecl@riverside.bardaglea.org.uk
Ext: 201123

Miss B MacKenzie
bema@riverside.bardaglea.org.uk
Ext: 201101

Miss C O'Keefe
chke@riverside.bardaglea.org.uk
Ext: 201008

Mr E Stubbles
elst@riverside.bardaglea.org.uk
Ext: 201008

1.0 INTRODUCTION

1.1 The purpose of this document is to present the E-Safety Policy for staff and students. It is also to ensure that all staff are aware of the appropriate steps to take when presented with an E-Safety issue. This policy is related to other policies including the safe use of ICT, anti-bullying and safeguarding to ensure the safety of all users.

1.2 Everyone has the right to access to the internet and all the benefits it offers. It is important that we prepare our young people for a world increasingly dependent on the use of technology in the home and workplace.

1.3 We, at Riverside Bridge School, are aware of the potential harm from some material that's exists on the Internet. The school will ensure that students will remain safe online through the use of safe filtering and parents are informed of use of computers in school and sign the internet use agreement form. Social media and the internet can provide a wide range of content, some of which is harmful. We as a school will take the steps outlined in this policy to support our staff and students in staying safe on-line.

2.0 WHAT IS E-SAFETY?

- E-safety is important to safeguard young people and adults in the digital world
- E-safety is about learning to understand and use new technologies and ICT in a positive and safe way.
- E-safety is not about restricting learning; it is about educating young people and adults of the risks as well as the benefits so they can feel confident and safe using technology.
- E-safety is about adults being educated to be able to support and help young people

3.0 POLICY

3.1 The Riverside Bridge School E-Safety Policy is one which provides clear direction to staff and others about expected behaviour when dealing with e-safety issues. This policy makes explicit the school's commitment to the development of good practice and sound procedures. It ensures that safeguarding concerns, referrals and monitoring may be handled sensitively, professionally and in ways which support the needs of the child.

3.2 Riverside Bridge School is committed to:

- Developing students behaviour towards, and respect for, other young people and adults, including freedom from bullying and harassment that may include cyber bulling.
- Supporting students' ability to assess and manage risk appropriately and to keep themselves safe online and through the use of technology.
- The provision of a broad and balanced curriculum that enables all students to achieve their full potential and make progress in their learning supported by the safe use of relevant technology.
- Engaging with parents and carers in the safe use of technology outside of school.
- Ensuring students know how to protect themselves online outside of school.

3.3 This E-Safety Policy has been written by the school, building on government guidance. All staff are reminded that e-safety should be consistent with the school ethos, other safeguarding policies and the Law.

4.0 TEACHING AND LEARNING

4.1 Internet use is part of the school curriculum and an important tool for learning; students use the internet widely outside school and need to learn how to evaluate internet information and to take

care of their own safety and security. The school internet access is designed to enhance and extend education and students will be taught what internet use is acceptable and what is not.

4.2 The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law; students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will use age-appropriate tools to research internet content.

4.3 E –safety skills will be specifically taught through the computing and ICT lessons and opportunities for reinforcement identified across the curriculum including but not limited to PSHE and life skills.

4.4 These lessons begin as part of any work using the internet.

- Students are encouraged to discuss their internet use and be open about their experiences.
- Students will be taught to use reputable search engines and be supported to critically evaluate the information they receive, at a level appropriate to their understanding.
- Students will be encouraged to report any content which makes them feel uncomfortable or unsafe.
- All screen time is to be overseen by a member of staff. Students should only use the internet, including on mobile devices where they can be monitored.
- Staff will receive training to support keeping our students safe on-line. This will include providing students with the skills to use the internet and social media safely outside school.
- Staff will be aware of and compliant to the school's E-Safety Policy and Acceptable Use Policy. New staff will be provided with these during induction.

5.0 MANAGING INFORMATION SERVICES

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- Images or videos that include students will be selected carefully and will not provide material that could be reused.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers is obtained when a student joins the school before any images/videos of pupils are electronically published or videoconferencing takes place.
- 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, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- 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.
- The school will control access to social media and social networking sites.
- If staff or students discover unsuitable sites, the URL will be reported to the School E-Safety Co-ordinator who will then record the incident and escalate the concern as appropriate.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- Videoconferencing will be supervised appropriately for the students' age and ability.
- Students will ask permission from a teacher before making or answering a videoconference call
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Parents and carers consent will be obtained prior to students taking part in video conferences.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Students will be instructed about safe and appropriate use of personal devices both on and off site.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

6.0 PERSONAL DEVICES

- Personal devices (such as mobile phones) brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device bought into school.
- Staff should not use their personal devices/phones when contacting pupils or parents: there should be access to a school phone.
- The taking, recording and sharing of images, video or audio on a personal device is forbidden. School devices are available for this purpose.

7.0 RADICALISATION

- In accordance to the Prevent policy, all staff have the responsibility for identifying staff/ students who have become at risk of radicalisation. Concerns can arise not only from use of school equipment but also content held on devices such as personal mobiles phones with internet access. Any content that causes concerns must be reported in line with the Safeguarding Policy.

8.0 USE OF DIGITAL IMAGES

- Parents/Carers should sign the digital media release form to give their consent before photographs are used.
- Digital media should be used in accordance with the home/school agreement.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks associated with publishing their own images on the internet e.g. on social networking sites.
- Pupil's full names should not be use anywhere on a website or blog, particularly in association with photographs.

9.0 CYBER BULLYING

- Cyber bullying is defined as bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.
- Cyber bulling differs from regular bullying because it can take place out of school and at any time of the day or night.
- Cyber bullying messages and images can be posted anonymously and distributed quickly to a very wide audience. It can be difficult and sometimes impossible to trace the source.
- All members of the school community are to be aware of bullying as an issue and must follow the guidelines in the school Anti-bullying policy, regardless of where or when the bullying has taken place.
- All incidents of cyber bullying reported to the school will be recorded.
- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyber bullying.
- There will be clear procedures in place to investigate incidents or allegations of cyber bullying.

10.0 POLICY DECISIONS

- All staff will read and sign the school Acceptable Use Policy before using any school ICT resources.
- Students will apply for Internet access individually by agreeing to comply with the school Student Acceptable Use Policy.
- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- 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.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- All users will be mindful of copyright issues and will only upload appropriate content onto school network drives.
- Only members of the current pupil and staff community will have access to the school network.
- Pupils/staff will be advised about acceptable conduct and use when using the school network.
- The school's senior leadership team and staff will regularly monitor the usage of the school network by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the senior leadership team. 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.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school acceptable use policy.

11.0 COMMUNICATIONS POLICY

- All users will be informed that network and Internet use will be monitored.
- An E–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The E–Safety Policy will be formally provided to and discussed with all members of staff.
- 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.

12.0 THE E-SAFETY OFFICER'S RESPONSIBILITIES

- Taking day to day responsibility for e-safety issues and having a leading role in establishing and reviewing the school e-safety policies/documents in conjunction with the Designated Safeguarding Lead

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Providing training and advice for staff
- Liaising with school IT technical staff
- Receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- Reporting regularly to Senior Leadership Team
- Undertaking regular e-safety training

13.0 STAFF RESPONSIBILITIES

- They have an up to date awareness of e-safety matters and of the current school E-Safety Policy and practices
- To ensure students are aware of all necessary measures to protect data and personal information
- To ensure students are critically aware of the materials they read and shown how to validate information before accepting their accuracy.
- They report any suspected misuse, problems or availability of inappropriate online material to the E-Safety Co-ordinator for investigation, action or sanction and inform the relevant staff (Class Teacher, Curriculum Pathway Leaders and Assistant Headteachers) at the earliest convenience
- To ensure that all digital communications with students (email or social media/networking should be on a professional level (in line with the School Acceptable Use Policy)
- To ensure that E-safety issues are embedded in all aspects of the curriculum and other school activities
- To ensure that E-Safety is promoted with the students in their care and they will be supported to develop a responsible attitude to safety online, system use and to the content they access or create.
- To ensure that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues relating to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- To ensure that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

14.0 STUDENT RESPONSIBILITES

- Maintaining a good understanding of how to research effectively and the need to avoid plagiarism and uphold copyright regulations
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Understanding school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on bullying through the use of technology
- Understanding the importance of adopting good e-safety practice when using digital technologies and social media/networking sites out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Ensuring they do not reveal personal details of themselves or others in online communication, or arrange to meet anyone without specific permission.

15.0 PARENT/CARER RESPONSIBILTIES

- Parents/carers who are reporting an online safety concern should report to the school in the first instance, who will follow procedures and attempt to resolve the incident. If this is not possible the incident may require referral to an outside agency.