Riverside School

E-Safety Policy

4 Appendices attached: *page*

1. ***Acceptable Use of the Internet and Emails by Staff*** ***10***
2. ***Unacceptable Use of the Internet, Emails or Social Media by Staff*** ***11***
3. ***Use of Social Media Protocols*** ***13***
4. ***Student Acceptable Use Agreement*** ***14***

This policy was approved at a meeting of the Governing Board on:
28 April, 2021

(Policy to be reviewed biennially)

Next review date – Spring term, 2023

E-Safety Policy

Introduction

This E-Safety Policy relates to other school policies including:

Safeguarding and Child Protection Policy, (February, 2019)
Anti-Bullying Policy, (March, 2018)

Also:

Ofsted. Inspecting e-safety in schools (April 2014)
DfE 'Keeping children safe in education', (September, 2020)
HM Govt 'Working together to Safeguard children' (March, 2015)
Ofsted 'Safeguarding children and young people and young vulnerable adults policy' (February, 2015)

Accountability

- Riverside's Governing Board recognises that establishing good E-Safety practice in the school is increasingly fundamental to the wellbeing of the students who can access the internet and social media. They are mindful of their responsibilities for monitoring the implementation of the policy and reviewing its effectiveness. This area of school life holds particular significance at Riverside, given the wide range of students' learning disabilities and vulnerabilities.
- The school's E-Safety Coordinator is the Computing Lead Teacher, who works closely with the school's Media Manager on E-Safety matters. Both are accountable to the school's DSLs, (Designated Safeguarding Leads).

Internet Use for Riverside students

- Riverside School recognises that most of our students are more vulnerable online due to a range of factors. This may include, but is not limited to students who are in care, students with SEND and mental health needs, students with English as additional language (EAL), and students experiencing trauma and/or loss.
- Riverside School ensures that differentiated and ability appropriate e-Safety and Digital Literacy education, access and support is provided to its students with the emphasis placed on developing social-emotional skills needed to navigate in the virtual world.
- Some students may be vulnerable to being bullied or to extremism/radicalisation through the internet, and they may not be able to recognise this. This is addressed in the schools Anti-Bullying Policy and our Prevent Duty documents. The school internet access is designed expressly for student use and includes filtering appropriate to the needs of our students.

Teaching and learning

- The internet is an essential element in 21st century life for education, employment, business, commercial and social interaction. The school recognises it has a duty to provide students with quality internet access as part of their learning experience, regardless of their learning disabilities and attainment levels.
- Use of the internet is also part of the statutory computing curriculum for those students in Team 1 and the higher-functioning students in Team 2.
- Computing is a necessary tool for staff and students. Riverside School ensures that students are included in this entitlement where appropriate, although they need a specialist approach to e-learning, as they do in other curriculum areas.
- The School implements E-Safety & Digital Literacy Plan, updated annually. The aim of this plan is to teach students how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.
- Students are taught about safe and appropriate electronic communication, including the indelible nature of emails, social media presence (balancing the virtual and real life), building safe and healthy relationships online.
- Aspect of e-Safety such as personal information protection, importance of maintaining strong passwords, avoidance of the cyberbullies and online predators (grooming), revenge porn and sexting, trolling and other harassment are carried in an age-appropriate way and in a way appropriate to students’ abilities, with emphasis on respecting oneself and others as well as becoming a positive role models and leaders.

Students are taught how to evaluate internet content

- The school ensures that the use of internet-derived materials by staff and students complies with copyright law.
- Students, who are able to, are taught how to report unpleasant internet content to school staff/adults or parents.
- Students, who are able to, are taught to identify and avoid fake news and questionable online content

Awareness and engagement with Parents/Carers

- Riverside School recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- Parents are supported by information on the safe use of the internet for their families where applicable.
- Riverside School seeks to provide information and awareness to parents by links to adequate websites sent on a regular basis. E-Safety Help Button will be added to the School’s website to guide parents where to get help if they have concerns.

- Parents' attention is drawn to the E-Safety Policy in newsletters, the School Offer and through information on the school website.
- Parents will be informed that they should supervise internet access at home to protect students from harm. Parents should check the PEGI age ratings on games to ensure that children do not consume age-inappropriate media.
- The school will offer support to parents to keep students safe online when outside school.

Information system security

- School IT systems, capacity and security are reviewed regularly.
- The school used anti-virus software and it is updated regularly.
- Security strategies are discussed with the Local Authority

Filtering and monitoring of the school internet

- Filtering: Riverside School uses the Rocket by LightSpeed Systems which is a sophisticated hardware package created exclusively for education that can screen an incoming web page to determine whether some or all of it should not be displayed to the user. The filter checks the origin or content of a web page against a set of rules provided by the school. The Computing Lead and Media Manager ensure that termly checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Monitoring: Our monitoring management app has the smarts to know when students are on unusual/suspicious browsing activity, notifying the IT/Media department in real time.
- The school works with the Local Authority and LGfL to ensure that all its IT systems set up to protect students are reviewed and updated as necessary.

E-mail

- Students are not given their own e-mail accounts on the school system, but where appropriate an approved email address for their use is set up for curriculum purposes that is monitored at all times by the class staff.
- Students of Team 1 will be given the O365 account provided by Microsoft; this type of account allows them to communicate only with other users of the O365 Riverside system.
- In an email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Student emails to an external organisation by students should be checked by a member of staff and authorised before sending.
- Staff should not use personal email accounts to communicate with service users.
- Staff should not use work email accounts for personal purposes.
- The forwarding of chain letters is not permitted.

Password Policy

- All members of staff have their own unique username and password to access our systems; members of staff are responsible for keeping them private.
- Team 1 and upper Team 2 students are provided with their own unique username and password to access their accounts to educational websites and are taught to keep them private.
- It is advised to all users to use strong passwords, keep them private; not to login as another user at any time; to log off or lock computers at all times when not in use.

Published content and the school website

- The contact details on the website are the school address, e-mail, telephone number and sometimes photos. Staff or students' personal information will not be published.
- The headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

Students' images and work

- Photographs that include students are selected carefully and will not enable individual students to be clearly identified without parental consent.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from for the use of photographs on the website is requested as part of the annual data collection process.

Social networking and personal publishing

- The School uses filtering software to block/filter access to social networking sites for students.
- Students are advised never to give out personal details of any kind which may identify them or their location or any other personal information.
- Students and parents are advised that the use of social network spaces outside school brings a range of dangers for our students.

Managing emerging technologies

- Emerging technologies are assessed for educational benefit and risk assessments are carried out before use in school is allowed.
- Staff should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting students within or outside of the setting in a professional capacity.
- Staff are not permitted to give their mobile phone numbers to students.
- Mobile phones and personally-owned devices are switched off or switched to ‘silent’ mode at school, unless permission has been given by the leadership team Bluetooth communication should be ‘hidden’ or switched off.
- If members of staff have an educational reason to allow students to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- In an emergency where a staff member doesn’t have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Students use of personal devices

- Students are educated regarding the safe and appropriate use of personal devices and mobile phone and are made aware of boundaries and consequences.
- The School expects student’s personal devices and mobile phones to be kept in a secure place and kept out of sight during lessons.
- Mobile phones or personal devices will not be used by students during lessons unless as a part of an approved and directed curriculum-based activity.
- Students of the Learning Centre, being 18+, are allowed to keep their mobile phones with them but are advised of the above.

Protecting personal data

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

Assessing risks

- The School takes all reasonable precautions to prevent access to inappropriate 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 a computer connected to the school network. Neither the school nor Haringey Council can accept liability for any material accessed, or any consequences of Internet access.
- The School will audit IT provision annually to establish if the E-Safety policy is adequate and that its implementation is effective.
- The School will ensure that monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

- All members of the community are made aware of the School's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

Handling E-Safety complaints

- Any complaint about staff misuse must be referred to the headteacher and if the alleged misuse is by the headteacher it must be referred to the chair of governors.
- Staff misuse that suggests criminal activity, or that a student has been harmed or that a member of staff is unsuitable to be with students is reported by the headteacher to the LADO.
- Students, parents, and staff are informed of the complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents/carers, and pupils to work in partnership to resolve online safety issues. After any investigation is completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes required.
- If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the local Safeguarding Team.
- Where there is suspicion, that illegal activity has taken place, the DSL will contact the local Safeguarding Team or Police if there is an immediate danger or risk of harm.

Community use of the internet

- The school will liaise with partnership schools and other local organisations to establish a common approach to E-Safety.

Introducing the E-Safety policy to students

- E-Safety rules, in a format appropriate for our students, are posted in classrooms and discussed with students as part of their learning, where appropriate.
- Students are informed that network and Internet use is monitored.
- E-Safety training is embedded within the Computing teaching and learning documents and the Personal, Social, Health and Economic Education (PSHEE) curriculum.
- Annual delivery of the e-Safety and the Digital Literacy Action Plan. This action plan is designed for the whole Riverside Community to engage with, in order to raise the profile of current and essential matters relating specifically to the digital world.

E-Safety staff training

- All staff are made aware of the School E-Safety policy, and training is delivered to all staff on the first training day of the school year annually.
- A copy of the policy is available on the school's website
- Staff are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Staff use of social media

- Staff are made aware that their use of social networking applications has implications for our duty to safeguard students.
- Students and their parents should not be accepted as friends by staff and any breach of this policy will result in disciplinary action being taken.
- All staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation (see Appendix 3 for further details).

Student use of social media

- The internet filtering restricts access to all social media for students. Students are not allowed to access social media at school.
- Students should not discuss their peers or employees of Riverside School on social media platforms.
- The minimum age for Facebook and other social media platforms is 13. Staff should report any underage use of social media as a safeguarding issue.
- See Appendix 3, Section 5 for further details.

E-SAFETY LINKS AND CONTACTS

CEOP (Child Exploitation and Online Protection Centre)	**https://www.ceop.police.uk/Safety-Centre/**
Child Exploitation and Online Protection (CEOP)	**www.thinkuknow.co.uk**
Childnet	**www.childnet.com**
NSPCC	**https://www.nspcc.org.uk/keeping-children-safe/online-safety/**
Childline	**https://www.childline.org.uk/**
UK Safer Internet Centre	**https://www.saferinternet.org.uk/**
Internet Watch Foundation	**https://www.iwf.org.uk/**
Internet Matters	**https://www.internetmatters.org/**

APPENDICES 1-4:

Appendix 1

Acceptable Use of the Internet and Emails by Staff

- All members of staff are responsible for explaining the rules and their implementations.
- All members of staff need to be aware of possible misuses of online access and their responsibilities towards students.
- The computer system is owned by the school, and may be used by students to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties, the students, the staff and the school.
- The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited and email sent or received.
- All Internet activity should be appropriate to staff professional activity or the student's education.
- Access should only be made via the authorised accounts and passwords, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is excluded.
- Users are responsible for all email sent and for contacts made that may result in email being reserved.
- Use for personal financial gain, political purposes or advertising is excluded.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is excluded.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is excluded.
- Violation of the above code of conduct will result in a temporary or permanent ban on Internet use.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

Appendix 2

Unacceptable Use of the Internet, Emails or Social Media by Staff

The purpose of this policy is to inform staff that any abuse of the internet, emails or social media in school, including bringing the school into disrepute, is treated extremely seriously with disciplinary action being taken that could lead to dismissal.
Where staff are allowed to use the Internet, it is on the clear understanding that abuse will not occur.
All Internet connections and access through the Council's ICT Network are logged and monitored.

'Abuse' includes:

- Accessing, displaying, downloading or disseminating pornographic or other 'adult' materials
- Posting information that may tend to disparage or harass others on the basis of gender, race, age, disability, religion, sexual orientation, political affiliation or national origin
- Uploading photographs of students on to the Internet is forbidden without prior permission from the head teacher.
- Publishing statements that are defamatory and could bring the school or Local Authority into disrepute
- Publishing information that is false or misleading concerning the school or Local Authority or any other company, organisation or individual that could bring the school or Local Authority into disrepute
- Any activity that breaches the Data Protection Act including publishing confidential or proprietary information of the school or Local Authority, or any of its customers or other business associates, on unsecured Internet sites such as Bulletin Boards or disseminating such information that might compromise its confidentiality
- Unauthorised publishing of information not related to the school or Local Authority
- Knowingly downloading, using, or distributing software or programmes from the Internet without verifying their operational integrity, e.g. the absence of computer viruses and breach of copyright
- Participating in any form of gambling and personal use of the Internet facilities without the specific consent of the Headteacher of the school
- The use of social networking sites in school is not permitted and staff should also be aware that, whilst using these sites outside of school, discussions re school activities / students / parents / colleagues is not acceptable and they should note that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 as well as other legislation.
- Staff should also note that use of the Internet may be a cost to the school. Authorised personal use should therefore be paid for according to the policy of the school

Appropriate/sensible use

1. Abide by the *Use of Social Media Protocols* (Appendix 3).
2. Ensure any technological equipment, (including your mobile phone) is password/ PIN protected.
3. Use professional online accounts/ identities if you wish to have online contact with service users, their families and other professionals.
4. Make sure that all publicly available information about you is accurate and appropriate
5. Remember online conversations may be referred to as 'chat' but they are written documents and should always be treated as such.

6. Make sure that you know the consequences of misuse of digital equipment.
7. If you are unsure who can view online material, assume it is public. Remember - once information is online you have relinquished control.
8. Switch off Bluetooth
9. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.

Inappropriate/do not…

1. Give your personal information to service users -students/ young people, their parents/ carers. This includes mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords etc.
2. Share your personal details with service users on a social network site
3. “Friend” service users on personal social networking profiles.
4. Use your own digital camera/ video for work. This includes integral cameras on mobile phones.
5. Play online games with service users.

Appendix 3

Use of Social Media Protocols

1. Introduction

Social media and social networking sites play an important role in the lives of many people. We recognise that sites bring risks, but equally there are many benefits to be reaped. This document gives clarity to the way in which social media/mobile phones are to be used by staff, students, governors, visitors and helpers at Riverside. It also provides guidance for parents.

There are four key areas:

- The use of social networking sites by students within school
- Use of social networking by staff in a personal capacity
- Comments posted by parents/carers
- Dealing with incidents of online bullying

2. The use of social networking sites by students within school

The school's acceptable use agreements outline the rules for using IT in school and these rules therefore apply to use of social networking sites. Such sites should not be used/accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate. Social Media sites to be used in school include blogging sites and Twitter. Parents will give permission for children to access these sites in school as well as permission for images of their child / child’s work to be included on the site.

In terms of private use of social networking sites by a child it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook and Instagram to name two. Where it comes to the attention of staff that children under 13 have such accounts, we will contact parents to inform them.

3. Use of social networking by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

- Staff must **never** add students as ‘friends’ into their personal accounts (including past students under the age of 16).
- Staff are **strongly advised** not to add parents as ‘friends’ into their personal accounts.
- Staff **must not** post comments about the school, students, parents or colleagues including members of the governing body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current national teacher's standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' (Safer Recruitment Consortium).
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

4. Comments posted by parents

Parents will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include; the prospectus, the website, the Riverside School Facebook page, newsletters, letters and verbal discussion.

School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion.

Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents must not post pictures of students, other than their own children, on social networking sites where these photographs have been taken at a school event.

Parents should make complaints through official school channels rather than posting them on social networking sites.

Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

5. Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's anti-bullying policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

In the case of inappropriate use of social networking by parents, the governing body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the complaints policy and will send a letter.

The governing body understands that, 'there are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged.' Furthermore, 'Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- expose (*an individual*) to hatred, ridicule or contempt
- cause (*an individual*) to be shunned or avoided
- lower (*an individual's*) standing in the estimation of right-thinking members of society or
- disparage (*an individual in their*) business, trade, office or profession.' (National Association of Headteachers)

6. Further Guidance and advice

Cyber bullying: Advice for headteachers and school staff (DFE)
https://www.google.co.uk/search?hl=en&q=social+media+policy+guidance+schools&meta=&gws_rd=ssl

NASUWT Advice
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking/NASUWT_007513

Appendix

LONDON
GRID FOR LEARNING

Riverside School

Student Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it, but I will show a teacher / responsible adult. I have read and understand these rules and agree to them.

Signed: *Date:*

LONDON
GRID FOR LEARNING

S	I will only use the Internet and email with an adult
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don’t like on a screen, I will always tell an adult

My Name:

My Signature: