Rivermead

Together on the road to success

E SAFETY POLICY

Reviewed Yearly

Signed _____
Date_____
REVIEW DATE: Nov 2018

E Safety Policy

Writing the e-safety policy

- The e-Safety Policy relates to other school policies including those for Safeguarding and Student Protection, Anti-bullying, Prevent Duty and Computing.
- The school's e-Safety Coordinator is the DSL Lead, who is accountable to the headteacher.
- This e-Safety Policy is informed by DfE guidance, including *'Keeping Students Safe in Education, 2016)*.

-

Internet Use for Rivermead students

SEN students are potentially more vulnerable and more at risk than others when using ICT:

- Those with learning disabilities may make literal interpretations of content which will affect how they respond.
- They may not understand some of the terminology used.
- Those with more complex needs may not always understand the concept of friendship and therefore trust others naively.
- They may not know how to make judgements about what information is safe to share. This can lead to confusion about trusting others on the internet.
- Some students may be vulnerable to being bullied or to extremism/radicalisation through the internet and they may not be able to recognise this.
- Some students may not appreciate how their own online behaviour may be seen by someone else as bullying.

Teaching and learning

The internet is an essential element in 21st century life for education, business 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. It is also part of the statutory computing curriculum and a necessary tool for staff and students. Rivermead School ensures that:

- Students are included in this entitlement, although they need a specialist approach to e-learning, as they do in other curriculum areas.
- The school Internet access is designed expressly for student use and includes filtering appropriate to the needs of our students.
- Students are taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Students are educated in the effective use of the internet.
- Parents are supported by information on the safe use of the internet for their families where applicable.

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.

Information system security

- School ICT systems, capacity and security are reviewed regularly.
- Virus protection are updated regularly.
- Security strategies are discussed with the Local Authority

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 are set up for curriculum purposes that is monitored at all times by the class staff.
- In an email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain letters is not permitted.

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 ensure 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 parents or carers 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 will 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.
- Students and parents are advised that the use of social network spaces outside school brings a range of dangers for our students.

Managing filtering

- The school will work with the Local Authority via an SLA to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the DSL Lead/Network Manager.
- The Network Manger will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Rivermead also has its own web filtering/monitoring system to product students, that is regularly reviewed/improved/updated.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and risk assessments are carried out before use in school is allowed.
- The senior leadership team 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.
- Mobile phones and personally-owned devices are switched off or switched to 'silent' mode at school, unless permission has been given by the 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 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 may 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.

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. The school can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT provision 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.

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.
- Any staff misuse that suggests a crime has been committed, a student has been harmed or that a member of staff is unsuitable to work with students are reported by the headteacher to the LADO.
- Students, parents and staff are informed of the complaints procedure.

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 and Health Education (PSHCE) curriculum.

Social networking

- 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.
- Staff should avoid bringing the school into disrepute when using social networks and any breach of this policy will result in disciplinary action being taken.

Staff emails

- Staff should not use personal email accounts to communicate with service users.
- Staff should not use work email accounts for personal purposes.

Staff and the e-safety policy

- All staff are made aware of the School e-safety policy and its importance explained.
- A copy of the policy are available in the staff room and on the school shared area.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention is drawn to the e-Safety Policy in newsletters, the School Offer and through information on the school Website.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website/VLE and on-line student records.
- their children's personal devices in the school (where this is allowed)

Prevent duty

- Rivermead School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.
- We protect children from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.
- Our Safeguarding, Prevent Duty and eSafety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.

Appendix 1 Internet Safety and Access

- 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.
- Staff, including those not directly employed by the school, requesting Internet access should sign a copy of this Acceptable Use Statement and return it to the School.
- 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 Statement for School Employees on the Abuse of the Internet

The purpose of this policy is to inform staff that abuse of the Internet in school are treated extremely seriously with disciplinary action being taken that could lead to dismissal
The policy should be read together with any school policy on use of the Internet
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

E-Safety Social Media Guidance

Appropriate

1. Set your privacy settings for any social networking site.
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

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. Use your personal mobile phone to communicate with service users. This includes phone calls, texts, emails, social networking sites, etc.
3. Use the internet or web-based communication to send personal messages to students/young people
4. Share your personal details with service users on a social network site
5. Add/allow a service user to join your contacts/friends list on personal social networking profiles.
6. Use your own digital camera/ video for work. This includes integral cameras on mobile phones.
7. Play online games with service users.

Appendix 3

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

Rivermead

Think before you click

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: