E-safety Policy

Change History

Date reviewed	Based on	Changes applied	Updated by
April 2017	Original	Added section on Cyber-bullying, Exploitation & Extremism.	E-safety Team
October 2015	Original	Incorporated all appendices in main policy. Changed e-safety coordinator to DSL. Added that staff are not allowed to use personal mobile phones to take photographs of pupils (sections 11.5 and 11.6)	Governing Body
April 15		Original	HT

Review: Annually **Next review**: April 2018

Ratified	Signed by Chair of Governors
21.10.15	

This policy is concerned with The Rise School's approach to e-safety.

This policy is to be implemented by:

- all staff

This policy is addressed to:

- all staff
- pupils
- parents

The purpose of this policy is to highlight the need to educate children and young people about the benefits and risks of using new technology, and to provide safeguards and awareness for users to enable them to control their online experiences.

E-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology.

The school will appoint an e-Safety coordinator. The Designated Safeguarding Lead will act as e-Safety coordinator.

This policy should be read in conjunction with the following policies:

- pupil behaviour policy
- anti-bullying policy
- child protection policy
- curriculum policy
- data protection policy
- security policy.

Guidance & procedures

Contents

15. Handing e-safety complaints

16. Communication of the policy

1. Why is Internet use important?

1.1 The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

1.2 Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

1.3 Many pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2. How does Internet use benefit education and enhance learning?

2.1 Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils world-wide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of Networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority and DCSF
- access to learning wherever and whenever convenient

2.2 The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

2.3 Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.

2.4 Internet access will be planned to enrich and extend learning activities.

2.5 Staff should guide pupils to on line activities that will support learning outcomes planned for the pupils' age and maturity.

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

2.7 See Appendix 2: E-Safety Rules for a description of acceptable and unacceptable computer use rules.

3. Good habits and dangers to consider

Good habits

3.1 E-Safety depends on effective practice at a number of levels:

- responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use
- safe and secure broadband from the provider including the effective management of content filtering
- Advice and guidance from National Education Network standards and specifications

Dangers to consider

3.2 Some of the dangers users 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 subject to grooming by those with whom they make contact on the Internet
- the sharing / distribution of personal images without an individual's consent or knowledge
- inappropriate communication / contact with others, including strangers
- cyber-bullying
- access to unsuitable video / Internet games
- an inability to evaluate the quality, accuracy and relevance of information on the Internet
- plagiarism and copyright infringement
- illegal downloading of music or video files#

- Radicalisation
- the potential for excessive use which may impact on the social and emotional development and learning of the young person.

3.3 As with all other risks, it is impossible to eliminate those dangers completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

3.4 Regular training and awareness will take place in classes for pupils along with Parent Meet sessions on E-Safety and INSET sessions for staff.

4. Authorised Internet access

4.1 All staff must read and sign Appendix 4: Acceptable ICT Use Agreement before using any school ICT resource and serves as a part of the induction paperwork for all employees and volunteers.

4.2 Parents will be informed that pupils will be provided with supervised Internet access.

4.3 Parents will be asked to sign and return Appendix 1: Acceptable ICT Use Agreement which will also be signed by pupils each year.

5. World Wide Web

5.1 If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-safety coordinator or network manager who will investigate and take appropriate action, liaising with broadband provider if necessary.

5.2 The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

5.3 Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

6. Email

6.1 Pupils may only use approved e-mail accounts on the school system.

6.2 Pupils must immediately tell a teacher if they receive offensive messages.

6.3 Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

6.4 Pupils may must not access others pupil's accounts.

6.5 Whole class or group e-mail addresses should be used in school.

6.6 Access in school to external personal e-mail accounts may be blocked.

6.7 E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

6.8 The forwarding of chain letters is not permitted

7. Social networking

7.1 Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.

7.2 Pupils will be advised never to give out personal details of any kind which may identify them or their location.

7.3 Pupils should be advised not to place personal photos on any social network space.

7.4 Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

7.5 Pupils and parents should be made aware that some social networks are not appropriate for children of school age.

8. Cyber-bullying, Exploitation & Extremism

8.1 Cyber-bullying like all forms of discrimination is not tolerated at The Rise School. Pupils are encouraged to report cyber bullying to the Senior Leadership or Behaviour team.

8.2 The school promotes positive online communication, counteracting cyber-bullying in all forms; dealing with incidents reported or detected.

8.3 The school promotes safe communication online, to counteract exploitation and extremism, through well-established systems for monitoring, developing of pupils understanding and reporting of concerns with relevant authorities.

8.4 The school will work in partnership with the LGfL to ensure filtering systems are as effective as possible.

9. Managing emerging technologies

9.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. This includes mobile phones, smart watches and any similar devices.

9.2 Mobile phones and other smart devices are not allowed in school. If a mobile phone or other smart device is brought in to school it will be kept in the school safe until the end of the day.

10. Published content and the school website

10.1 The contact details on the website should be the school address, e-mail and telephone number.

10.2 Staff or pupils personal information will not be published.

10.3 The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

11. Publishing pupils' images and work

11.1. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified on the website.

11.2. Pupils' full names will not be used anywhere on the website or Blog, particularly in association with photographs.

11.3. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or used on Social Media. See Appendix 3: Parental Consent Form

11.4. Work can only be published with the permission of the pupil and parents.

11.5. Staff will use only school equipment to take photographs of pupils. Staff will ensure that the safe and appropriate use and storage of the equipment and memory cards containing any images of pupils is maintained. All images are to be stored securely on the school system as soon as possible from the time of use and deleted from the equipment and memory cards before the next use.

11.6. The use of personal devices (e.g. mobile phones, cameras) to take images of pupils is strictly forbidden.

12. Information system security

12.1 School ICT systems capacity and security will be reviewed regularly.

12.2 Virus protection will be installed and updated regularly.

12.3 Security strategies will be discussed with our technical support team and broadband provider if necessary.

13. Protecting personal data

13.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

14. Assessing risks

14.1 The school will take all reasonable precautions to prevent access to inappropriate material.

14.2 However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

14.3 The school will audit ICT use routinely to establish if the e-safety policy remains adequate and that the ongoing implementation of the e-safety policy is appropriate. See Appendix 6: E-safety audit

15. Handling e-safety complaints

15.1. Complaints of Internet misuse will be dealt with by a senior member of staff.

15.2. Any complaint about staff misuse must be referred to the Headteacher.

15.3. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

15.4. Pupils and parents will be informed of the complaints procedure.

15.5. Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures.

16. Communication of the policy

Pupils

16.1 Pupils will be reminded of the Rules for Internet access, as detailed in Appendix 1.

16.2 Pupils will be informed that Internet use will be monitored.

16.3 Differentiated acceptable use and e-safety expectations will be displayed prominently in classrooms near stationary computers for pupil usage in a way that pupils can access.

Staff

16.3 All staff will be given the school e-safety policy and its importance will be explained.

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

Parents

16.5 Whole community engagement is paramount in ensuring that the safe use of technology is communicated to all. Parents need to play the pivotal role in educating their children about staying safe while using a variety of different technologies as the school cannot apply filters or secure IT access out of the school environment. Parents' attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school website.

Appendix 1:
Acceptable ICT use agreement (pupils and parents)

The following letter will be sent to new pupils and their parents

Rules for responsible computer and Internet use

In school we have access to the Internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. We at The Rise School are aware that young people should have an entitlement to safe Internet access at all times. However, the school and parents have a duty of care to protect children and ensure that Internet use is responsible and safe.

The school strongly recommends that primary age children do not use social network sites such as Facebook and Bebo at home as these sites carry an age-restriction and pose a risk to children.

Social networks have no place in our school and so school staff should not be approached online or invited to join.

Please read and sign the 'Rules for Responsible Computer and Internet Use' with your child to show your support of the school in this important aspect of our work.

- I will only access the system with my own login.
- I will not access other people's files.
- I will ask permission from a member of staff before using the Internet and I will only access sites approved by a trusted adult.
- I will only email or message people I know or a trusted adult has approved.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number in any message.
- I will report any unpleasant material, anything that upsets me or anything that seems 'wrong'. I will tell a trusted adult if I am contacted by a stranger or receive unpleasant messages. I understand that this would help protect other pupils and myself and that the school would need to take appropriate action.
- I understand that the school may check my computer files and may monitor my use of the internet.
- I will not being a personal computer or smart device into school without permission from my class teacher.

Sanctions:

- deliberate minor incidents in school will lead to a warning
- serious incidents (or repeated minor incidents) will mean access to the ICT equipment or the Internet is removed
- illegal behaviour by anyone will be dealt with by the police

Parent/Guardian Name _____

Parent/Guardian Signature _____

Pupil Name _____

Pupil Signature _____

Date _____

Appendix 2: E-safety rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use:

- the school owns the computer network and can set rules for its use
- it is a criminal offence to use a computer or network for a purpose not permitted by the school
- irresponsible use may result in the loss of network or Internet access
- network access must be made via the user's authorised account and password, which must not be given to any other person
- all network and Internet use must be appropriate to education
- copyright and intellectual property rights must be respected
- messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers
- anonymous messages and chain letters are not permitted
- users must take care not to reveal personal information through email, personal publishing, blogs or messaging
- the school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission
- use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix 3: Parental consent form

To be sent home and returned with the Acceptable ICT use agreement and the E-Safety rules.

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-safety rules have been understood and agreed.

Parent's consent for Web publication of work and photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's consent for Internet access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but that the school cannot be held responsible for the content of materials accessed through the Internet.

Signed:

Please print name:

Date:

Please complete, sign and return to the school

Appendix 4: Acceptable ICT use agreement (staff)

To ensure that all staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

Monitoring

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

LGfL (London Grid for Learning) will monitor and audit Internet use to see if users are complying with the policy. Any potential misuse identified by LGfL will be reported to the school.

N.B. Access to any site that might be deemed 'inappropriate' but has an educational use should be recorded in your planning.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of children, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative
- material that breaches the Obscene Publications Act in the UK
- criminally racist material.

If inappropriate material is accessed accidentally, users should immediately report this to the LGfL.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand that comments made in networking sites such as Facebook or Bebo should make no direct or indirect reference to our school, should not include images of school or children involved in school activities. Parents of children in our school will not be approached or contacted through social networks, and any requests to become online 'friends' with pupils or parents will be refused.
- I will not bring personal computers or devices into the school without explicit permission from the Headteacher.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ……

Print Name: ……

Date: ……

Appendix 5: E-safety audit

This quick self-audit will help the senior leadership team (SLT) assess whether the safety basics are in place:

Has the school an e-Safety Policy that complies with CYPD guidance?	
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
The Policy is available for parents:	
The E-Safety Coordinator is:	
Is E-Safety training provided for all staff and pupils?	
Do all staff sign an ICT Code of Conduct on appointment?	
Are the E-Safety rules for pupils displayed in all rooms with computers in?	
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	
Has the school filtering policy been approved by the SMT?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Broadband monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

- Surveys / questionnaires of – pupils – parents/carers - staff