Rainow Primary School

Caring, Learning, Achieving.

e-Safety Policy

Members of staff responsible:	**Mr Norris / Mr Trueman (SL)**
Date approved by Governors:	**Summer 2021**
Date to be reviewed:	**Summer 2024**

Introduction

This e-Safety Policy encourages the responsible use of electronic communication through education and good practice. It highlights the benefits and risks of these technologies and sets expectations of behaviour. The guidelines set boundaries that enable control of the on-line experience without denying children the opportunity to broaden their learning experience. This document focuses on those factors under control of the school.

Good Habits

e-safety is a core element of the school's safeguarding system and online 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 the e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband provided by Schools Broadband, a specialist Education Internet Service Provider (ISP). Schools Broadband also provide effective management of content filtering as part of the school's subscription. The content filtering system used is Netsweeper, which facilitates restrictive settings for different user profiles.

Scope

This policy will:

- Be checked annually.
- Form the basis of good e-Safety practice within the school.

Teaching and Learning

E-safety should be a continuing focus in all areas of the curriculum and staff should reinforce e-safety messages, wherever possible, in the use of Computing across the curriculum.

- The school will provide internet access as part of the learning experience provided by an educational broadband network.
- The school's internet access will be employed expressly for education and will include age-appropriate content filtering.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and learning activities. The school will also promote and take part in the annual Safer Internet Day https://www.saferinternet.org.uk/ which takes place in February each year.
- A planned online safety curriculum should be provided as part of Computing / PHSE /other lessons and should be regularly revisited throughout the academic year.

- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to be critically aware of the online materials they read and shown how to validate information before accepting its accuracy.
- The school will ensure that the use of internet derived materials by staff and pupils complies with the law.
- The Digital Leaders, selected pupils from KS2 who champion, support and help lead Computing in school, will seek to model and promote good internet use.
- School will seek to provide information and awareness to parents and carers through letters and newsletters, parent workshops and reference to relevant online guidance provided by the school website.
- The Computing Subject Leader will ensure that this policy is applied.

Pupil Responsibilities

- Pupils must keep their personal passwords safe and not share them with other pupils.
- In school, pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive messages or see inappropriate materials.
- Pupils should ask permission from the supervising teacher before making or answering a voice or video conference.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- 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 when using social networking sites and or digital learning platforms.
- Pupils must not arrange to meet anyone without specific permission.

The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe online. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well-being of any pupil is being compromised.

Published Content

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs and/or videos of pupils are published on the school website, Twitter feed or digital learning platforms**.**
- Pupils' full names will not be used anywhere on the school's online sites.
- Social networking sites will be filtered or blocked at the discretion of the Headteacher.
- Newsgroups / forums will be blocked unless a specific use is approved.

- Staff are advised of the possible consequences and repercussions of any information that they make available online, for example on a social networking site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils.

Filtering Content

- The school will work with the LA to ensure systems to protect pupils are reviewed and improved. The content filtering system used is Netsweeper, which facilitates restrictive settings for different user profiles.
- If staff or pupils discover an unsuitable site, it must be reported to the Computing Subject Leader.
- Virus protection will be installed on every computer and will be set to update automatically at least once a week.
- IP video conferencing should use the educational broadband network to ensure quality of service and security.

Introducing Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will be used only at the discretion of the Headteacher.
- The use of portable media will be monitored closely as potential sources of computer viruses and inappropriate material.
- Staff will not use personal equipment or non-school personal electronic accounts when contacting students. Staff will only use the school phone, school email or school's digital learning platforms where contact with pupils and/or parents is required.

Policy Decisions

- All staff must read and sign the *'Staff Acceptable Use Policy'* agreement before using any school ICT resource. (see Appendix 1)
- Pupils must have read (with the class teacher), understood and agreed to the 'Pupil Acceptable Use Policy' at the beginning of each school year (see Appendix 2a and 2b for examples of what the children must agree to at Rec/KS1 and KS2). This may take the form of classes creating a 'Class Charter/Agreement'.
- The Digital Leaders will take a role in reviewing the *'Pupil Acceptable Use Policy'* and will also present an assembly to relaunch it annually.
- Parents will be asked to agree to and return a *'Parent/Carer Acceptable Use Policy'. (See Appendix 3).* This will normally be done during the new starter induction process.
- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of internet access. Any inappropriate sites will be immediately reported to our private broadband provider and / or local authority ICT team.
- The school will audit ICT provision annually to establish if the e-safety policy is adequate and that its implementation is effective.

Handling Incidents

- Incidents of Internet misuse, either by pupils or staff, will be dealt with by the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection/safeguarding procedures.

Policy Communication

- e-safety rules will be posted in all networked rooms and, as minimum, discussed with the pupils at the start of each year.
- Pupils will be informed that network and internet use will be monitored.
- All staff will be given access to the School e-safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Parents will be advised that the e-safety policy is published on the school web site and is also available in hard copy by application to the school.

Useful Advice/Support
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
https://www.saferinternet.org.uk/
http://swgfl.org.uk/products-services/esafety/resources
https://360safe.org.uk/

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

Child Protection and Safeguarding Policy
Social Media Policy
Behaviour, Discipline and Anti-bullying
Data Protection / GDPR Policy

Appendix 1 – Staff ICT Acceptable Use Policy Agreement

Staff ICT Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work. The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that the young people receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE, iPads, etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher, Deputy Head or Computing Subject Leader.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will only use my personal equipment to record these images if it is password protected.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.

- I will only communicate with young people and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- If the data on any device is breached, I will report it to the Headteacher, Data Protection Officer, Deputy Head or Computing Subject Leader.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand-held / external devices (iPads/PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand the importance of regularly backing up my work.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. • I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school GDPR Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that any staff or young person's data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- It is my responsibility to understand and comply with current copyright legislation.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name:

Signed: **Date:**

Appendix 2a – Rec / KS1 Acceptable Use Policy Agreement

Rainow Primary School
Caring, Learning, Achieving

KS1 Pupil Acceptable Use Policy Agreement

Our aim:

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- Always keep my passwords a secret.
- Only open pages which my teacher has said are OK.
- Only work with people I know in real life.
- Tell my teacher if anything makes me feel scared or uncomfortable on the internet.
- Make sure all messages I send are polite.
- Show my teacher if I get a unkind message.
- Not reply to any unkind messages or anything which makes me feel uncomfortable.
- Only email / message people I know or if my teacher agrees.
- Only use emails / messaging which the school allow.
- Talk to my teacher before using anything on the internet.
- Not tell people about myself online (I will not tell them my name, anything about my home , family and pets)
- Not upload photographs of myself without asking a teacher.
- Never agree to meet a stranger.
- Look after and respect the school ICT equipment.

I know that:

➢ **Anything I do on the computer may be seen by someone else.**

➢ **The CEOP report button is there to keep me safe online and I know when to use it.**

Appendix 2b - KS2 Acceptable Use Policy Agreement

Rainow Primary School
Caring, Learning, Achieving

KS2 Pupil Acceptable Use Policy Agreement

Our aim:

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- Always keep my passwords a secret.
- Only use, move and share personal data securely.
- Only visit sites which are appropriate.
- Work in collaboration only with people my school has approved and will deny access to others.
- Respect the school network security.
- Make sure all messages I send are respectful.
- Show a responsible adult any content that makes me feel unsafe or uncomfortable.
- Not reply to any nasty message or anything which makes me feel uncomfortable.
- Not use my own mobile device in school unless I am given permission.
- Only give my mobile phone number to friends I know in real life and trust.
- Only email / message people I know or approved by my school.
- Only use email messaging which has been approved by the school.
- Discuss and agree on my use of a social networking site with a responsible adult before joining.
- Always follow the terms and conditions when using a site.
- Always keep my personal details private. (my name, family information, the journey to school, my pets and hobbies are all examples of personal details)
- Always check with a responsible adult before I share images of myself or others.
- Only create and share content that is legal.
- Never meet an online friend without taking a responsible adult that I know with me.

I know that:

➢ **The CEOP report button is there to keep me safe online, and I know when to use it.**

➢ ***Anything I share online may be monitored.***

➢ ***Once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.***

Appendix 3 –Parent / Carer ICT Acceptable Use Policy Agreement

Rainow Primary School
Caring, Learning, Achieving

Parent/Carer - ICT Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of eSafety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement can be found as an appendix of the School e-safety policy.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent Permission Form

Parent/Carer's Name:

Pupil Name:

As the parent/carer of the above pupil(s), I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed: **Date:**