Chalk Ridge Primary School

E-Safety Policy

Agreed and adopted: September 2016
Reviewed: October 2020
May 2021

Next review: May 2022

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Curriculum, Child Protection and PSHE.

Our e-Safety Policy has been built on County and Government guidance. It has been agreed by the staff, senior leadership team and approved by governors.

The e-Safety Policy will be reviewed annually.

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

- Responsible ICT use by all staff, governors 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 including the effective management of content filtering.

Aims and Objectives of Internet Use

Why is Internet Use Important?

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.

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

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.

How does internet use benefit education?

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.

How can internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Through our online learning platform 'Purple Mash' and through our school website, pupils can access homework and home learning tasks to further understanding and support them in meeting learning outcomes planned for their year group

E-Safety and the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis, using age appropriate resources from *UK Safer Internet Centre, Childnet* and the *Google – Be Internet Legends* programme of study. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We regularly monitor and assess our pupils' understanding of e-safety.

- The school provides opportunities within a range of curriculum areas and discrete Computing lessons to teach about e-safety (in accordance with the medium term planning.)
- Educating pupils on the dangers of technologies that maybe encountered outside school may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP/NSPCC report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

Acceptable ICT use

Authorised Access

- All staff, governors and pupils must follow the ‘Acceptable ICT Use’ sections of this policy.
- Parents will be asked to sign and return a ‘Pupil Acceptable Use’ form (see Appendix C) on behalf of their child/ren on admission to the school.
- Staff and Governors will be asked to sign and return a ‘Staff and Governors Acceptable Use’ form (see Appendix D) on beginning employment at Chalk Ridge Primary School.

World Wide Web

- If staff, governors or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Computing subject leader or network manager who will contact the Local Authority helpdesk to block said site.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Social Media

As a school we recognise that social media and networking are playing an increasing role within everyday life and that many staff and governors are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff, governors and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

As a school we block access to social networking sites on all school computers.

Staff and governors should:

- ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc. Security settings should be checked regularly.
- not accept current or ex-pupils as ‘friends’ on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members live and have friends within the local community and ask that these members of staff take extra care when posting online.
- ensure that their communication maintains their professionalism at all times.
- be aware that electronic texts can be misconstrued so should endeavour to minimise the possibility of this happening.
- not use these media to discuss confidential information or to discuss specific children.
- check with the Computing subject leader or ICT technician if they need advice on monitoring their online persona and checking their security settings.

Social media sites have minimum age limits and pupils should not be accessing content through social media apps/websites that has a minimum age limit above that of their own age. Guidance for this can be found on the school website page, ‘Internet and online safety.’ We recognise that some are signed up for with, or without, parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will ensure that parents are aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children’s accounts should any issues, such as cyber-bullying occur.

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Managing Emerging Technologies/ Future developments

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. This policy will be amended as required.

Use of Memory Sticks (and other portable storage)

All teaching staff have an encrypted memory stick for use as described in the 'Staff and Governor Acceptable Use Agreement'. In addition to this, staff will be told to minimize storage of sensitive and/or confidential information (e.g. reports, PLPs) on these devices.

Personal Mobile Phones and Mobile Devices

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity

Published Content and the School Web Site

- The school website complies with statutory DfE requirements.
- The contact details on the Web site include the school address, office and staff e-mail addresses and telephone number.
- Staff, governors or pupil's personal information will not be published.
- The network manager, head teacher, deputy head teacher, office staff and Computing subject leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

Virtual Learning Platform and Home Learning

- The school subscribes to Purple Mash as an online platform that allows children to access homework and home learning tasks from home.
- Login details and passwords will be provided annually. There is a clear expectation set that these must not be shared with others.
- In the event that it is required children's learning must take place from home, home learning tasks are shared via the school website or Purple Mash, providing enriching and

meaningful activities appropriate to each child's age/ability; supporting them in achieving learning outcomes relevant to their year group.

Publishing Digital and Video Images

We follow these rules to maintain safety on our school website:

- For a photograph of a child to appear on the site, consent must have been gained from the parent or guardian of the child. This consent is sought on admission and reviewed annually. A parent or guardian may choose to withdraw permission at any time.
- If we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure they are not left out of situations unnecessarily.
- We will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.
- If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason. (See above.)
- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
- Personal information about children or staff is not shared on our website. Contact e-mails are provided only for the School office.
- All information on the school website is published by the website administrator, even if it is not written by him/her. This avoids content on the website inadvertently contravening these rules.
- Photographs of swimming, changing for PE and other instances deemed inappropriate by class teacher will not be taken.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. 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. Neither the school nor Hampshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should review ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. This policy is reviewed annually, with termly health checks.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

E-safety incidents will be responded to in accordance with the flowchart in Appendix A.

In the event that staff are made aware of incidents of misuse that occur between pupils (including their communication through mobile devices and social media platforms) or any other matters relating to e-safety that raise concerns around our pupils use of technology outside of school, the following procedure shall be followed:

1. Incident reported to member of staff.
2. Class teacher to speak to any pupil's involved and record information provided.
3. Parents will be informed of the incident.
4. Parents will be guided to relevant materials (via the school website) in order to help support their child with any relevant e-safety concerns.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms (see Appendix B) and through Computing lessons.
- Pupils will be informed that Internet use will be monitored.
- Sign 'Acceptable Use' agreement.

Staff and Governors

- All staff and governors will be given the School e-Safety Policy and its importance explained.
- Staff and governors should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Sign 'Acceptable Use' agreement.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web-site.

We can check that this is working by:

Talking with children and parents
Discussion at staff meetings to identify impact of policy and identify next steps if and when required

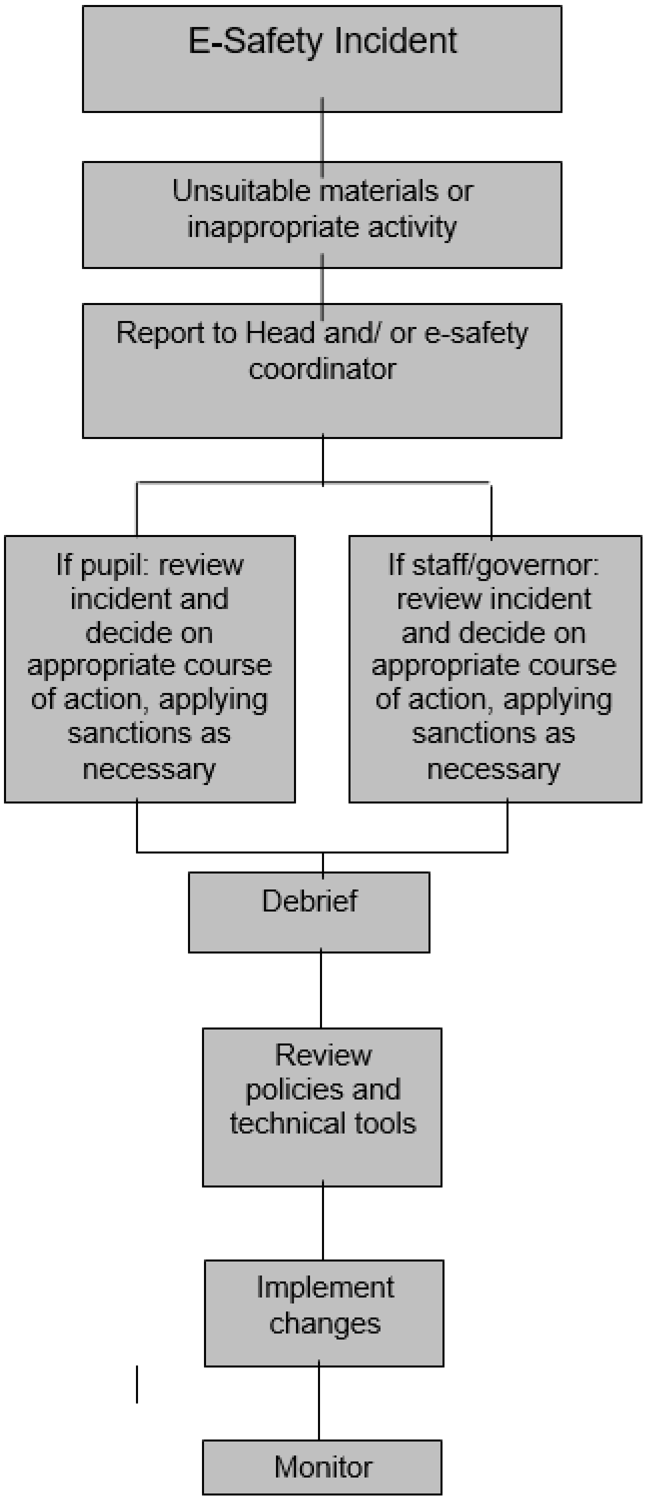
Responding to e-safety incidents – Appendix A

E-Safety Rules for KS1 and KS2 – Appendix B

Pupil Acceptable Use Policy – Appendix C

Staff and Governors Acceptable Use Policy – Appendix D

Appendix A


E-Safety Incident
Unsuitable materials or inappropriate activity
Report to Head and/ or e-safety coordinator
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff/governor: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief
Review policies and technical tools
Implement changes
Monitor

Appendix B

Key Stage 1

Think then Click

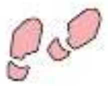
These rules help us to stay safe on the Internet:

- We only use the internet when an adult is with us.

- We can click on the buttons or links when we know what they do.

- We can search the Internet with an adult.

- We always ask if we get lost on the Internet.



Key Stage 2

Think then Click

- We ask permission before using the Internet.
- We tell an adult if we see anything we are uncomfortable with.
- We send e-mails and messages that are polite and friendly.
- We never give out personal information or passwords but we can share them with our parents
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

Appendix C

Pupil Acceptable ICT use

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 head teacher 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 web-sites, 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.

Signed:……………………………………………………. Date:…………………………………

Appendix D

Staff and Governors Acceptable ICT Use
Staff Information Systems Code of Conduct

Purpose: To ensure that staff and governors are fully aware of their professional responsibilities when using information systems. Staff and governors should consult the school's e-safety policy for further information and clarification.

- 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 rôle.
- 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 one of the Designated Safeguarding Leaders.
- 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.

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.

Signed:…………………………………….   Date……………………………