Rydon Primary School

ICT – E-Safety

Policy and Guidelines

C Nevinson

V Horton

December 2016

E-Safety Policy

Rationale

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

Unfortunately, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images, video games, internet games or other content including: sexual exploitation; radicalisation and sexual predation.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact with 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.
- 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.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the "offline world" and it is essential that this E-Safety Policy is used in conjunction with other school policies (e.g. Managing Behaviour, including bullying/racism, Child Protection and Data Protection policies).

As with all other risks, it is impossible to eliminate those risks 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.

Development / Monitoring / Review of this Policy

- This e-safety policy has been developed by the: ICT Team and governors.
- Consultation with the school community has taken place through: staff meetings; parents via newsletters and website; pupils through curriculum teaching and e-safety days.
- It is to be reviewed annually by the ICT/E-safety Leader.
- The implementation of the policy will be supported and monitored by the ICT/E-safety Leader and the ICT Team.

Scope

This policy applies to all members of the school community including staff, pupils, parents/carers, visitors, community users who have access to, and are users of, the school ICT systems both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies, and will (where known) inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school. Any such incidents will be recorded in the E-safety Log Book.

Technical/infrastructure/equipment

- All users will have clearly defined access rights to school ICT systems.
- Users will be made responsible for the security of their username and password, and must be vigilant about allowing other users to access the systems using their log on details.
- The school maintains and supports the managed filtering service currently provided by SWGfL. Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Team.
- Personal data about staff or pupils cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- USB devices and CD-ROMs may only be used on the Network after having been virus checked.
- The ICT Technician is able to monitor the activity of users in suspicious circumstances on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- The master/administrative passwords for the school ICT system, used by the ICT Technician, are also available to the Headteacher and ICT Leader and a copy is kept in the school safe.

- Users are to report any actual/potential e-safety incident to the ICT Technician who will inform the E-safety Leader and Headteacher. Any incident which requires action to be taken will be recorded in the E-safety Log Book.

Curriculum/Pupil Use

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
- A planned e-safety programme, Digital Literacy and Citizenship, is provided as part of Computing / PSHE curriculum and will be regularly revisited by the pupils to learn the risks of e-communication (personal details, viruses, phishing, cyber-bullying, Internet risks, copyright, longevity of posted information/images etc).
- Key e-safety messages are reinforced during e-safety days and e-safety assemblies.
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Upper KS2 Pupils should be helped to understand the need for the Pupil Acceptable Use Policy Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- During Computing lessons, pupils will be made critically aware of plagiarism, quality, accuracy, bias and relevance of information. This work will be followed up when cross-curricular opportunities arise.
- Pupils may only use computers/digital resources under the supervision of a member of staff although the adult may not necessarily be standing over them. Pupils are expected to use computer responsibly giving consideration to the SMART rules, and for Upper KS2 the Acceptable Use Policy.
- Pupils may only use the Internet to search for resources to use in school work.
- The use of websites for other purposes; i.e. to play games, is only permitted by prior agreement with a member of staff. Lunch Clubs may only access approved sites.
- Pupils are made aware of the risks associated with searching using Google Images and are taught to immediately inform an adult if an inappropriate image is viewed. ***Pupils not using computers responsibly will be denied freedom of access.***
- Pupils must be advised as to the social, health and emotional impact of the excessive use of e-technologies.

Images

- Personal images/video in pupil folders should only be stored on the school network and can only be accessed beyond school via encrypted and password protected means.
- Publication of video/still images is subject to the approval of the participants and where appropriate, parents/guardians.
- Images of pupils/use of names may not be published for access externally without the permission of the Headteacher/Deputy Head, unless covered by the Digital Image Consent Form.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Information

- Pupils may only take digital information from school (via USB) with the permission of a member of staff. The information should be focused on learning.

Communication

- Pupils are taught about digital communication (email, social networking, chat) safety issues. The risks might include the use of personal details and conversing with strangers. They are also taught strategies to deal with inappropriate digital communication and are reminded of the need to write communications clearly and correctly, and not include any unsuitable or abusive material.
- Users must immediately report the receipt of any digital communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such digital communication.
- All incidents must be reported by the pupil to the class teacher, who can inform the ICT/E-safety Leader, ICT Technician and Headteacher, if appropriate.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, etc) must only take place on official (monitored) school systems.

Monitoring and Review

- Incidents of inappropriate use will be reported to the ICT Technician and ICT/E-safety Leader, and reported Headteacher. Incidents that require action to be taken will be recorded in the E-Safety Log Book.
- Staff will be kept up to date with developments via staff meetings/training.

E-Safety - Roles and Responsibilities

Governors – are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher – responsible for ensuring the safety (including e-safety) of members of the school community.

ICT Subject / E-Safety Leader - has a leading role in establishing, monitoring and reviewing the school e-safety policies / documents. Is responsible for raising awareness and addressing training/teaching of the whole school community

Pupils are responsible for using the school ICT systems in accordance with the Acceptable Use Policy for Pupils

Parents / Carers – endorse by signature the Digital Image Consent form and Pupil Acceptable Use Policy for Upper KS2. Parents will receive information about E-Safety via the school website, letters and related publications.

.

ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- there will be regular reviews and audits of the safety and security of school ICT systems.
- servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate, current virus checking devices and firewalls are in place.
- the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher
- takes day to day responsibility for e-safety issues

School Staff (teachers and support staff) are responsible (as relevant) for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy.
- e-safety issues are embedded in the curriculum and other school activities
- pupils understand and follow the school e-safety SMART Rules and where appropriate the Pupil Acceptable Use Policy

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- processes are in place for dealing with any unsuitable material that is found in internet searches.
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, USB sticks, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- **Data** is stored securely, computers are logged off after use and data is not transferred externally without having a secure password or being encrypted. Only legal copies of software are used with the consent of the ICT Technician, after being virus checked.

Supporting Policies + Documents

Staff Acceptable use Policy
Upper KS2 Pupil Acceptable use Policy
General Consent Form
Mobile Phone Policy