Warmsworth Primary School

Mill Lane, Warmsworth, Doncaster DN4 9RG
Telephone: 01302 852200   Facsimile: 01302 855454

E-Safety Policy

Writing and reviewing the e-Safety Policy:

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Anti-Bullying, Behaviour and Rewards and for Safeguarding:

- The school has a designated E-Safety Coordinator, who is also the Designated Child Protection Coordinator. There is close liaison between the e-Safety Coordinator and the Computing Coordinator.
- Our e-Safety Policy has been written by the school, building on previous policies and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: The Computing co-ordinator on behalf of the Governing Body.
- It was approved by the Governors on 18th October 2016.

E-safety Policy:

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming and related forums
- Mobile/ Smart phones with text, video and/ or web functionality

- Kindles, tablets, laptops and other mobile devices with web functionality.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. Risk may include the content available for view, contact made as well as personal conduct.

At Warmsworth Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Online safety is a concern for everyone. Pupils, teachers and parents in the wider school community should all work collaboratively to prevent online bullying and to develop a safe and positive attitude towards technology and online engagement.

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 policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure connectivity including the effective management of content filtering.

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;
- Provides a stimulus for cross-curricular learning in particular the use of media for literacy and the availability of rich and varied texts for reading;
- 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 DfE; 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 by Yorkshire and Humberside Grid for Learning.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Digital literacy and citizenship are included in a clear and progressive curriculum, to ensure that pupils understand how to conduct themselves online in a safe and appropriate manner. Pupils will be taught what comments are acceptable on social media via the modelling of posts on the Virtual Learning Environment.
- Internet access will be planned to enrich and extend learning activities in all curriculum areas.
- 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.

Authorised internet access:

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource (see Appendix A).
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access.

Information systems security:

- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Local Authority helpdesk via the e-Safety Co-ordinator or Computing Co-ordinator (see Appendix B).
- 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 (see Computing Curriculum).
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be monitored and updated regularly.
- Security strategies will be discussed with DMBC and the e-learning team.

Online Communication:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail or message.
- Pupils must not reveal personal details of themselves or others in electronic communication, or arrange to meet anyone.
- Whole class or group e-mail addresses should be used in school.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

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:

- 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 not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

Published Content and the School Web Site:

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published (unless logged in as a VLE user under a secure network).
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work:

- Photographs that include pupils will be selected carefully using parental permission slips and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the web site or VLE without parental permission (unless logged in as a VLE user under a secure network).
- Work can only be published with the permission of the pupil and parents using parental permission slips.

Social networking and personal publishing:

- The school, in collaboration with the internet service provider, will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of some social network spaces outside school is inappropriate / illegal for primary aged pupils.
- The school will work alongside outside agencies to educate parents about the potential risks and solutions to reduce these.

Cyber-bullying:

Cyber-bullying is the use of ICT, particularly mobile phones and the internet, deliberately to upset someone else. The school and wider community has a duty to protect all its members and provide a safe, healthy environment to promote a positive attitude towards technology and online engagement. The Educations and Inspections Act 2006 states that Headteacher's have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

Cyber-bullying is achieved through a variety of devices:

- Text messages - that are threatening or cause discomfort.
- Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed;
- Mobile phone calls - silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails - threatening or bullying emails, often sent using a pseudonym or somebody else's name;
- Instant messaging (IM) - unpleasant messages sent while children conduct real-time conversations online using a variety of software;
- Chat rooms - menacing or upsetting responses to children or young people when they are in web-based chat rooms or on social networking sights;

Forms of cyber-bullying include:

- Impersonation - breaking into an email or social networking account and using that person's online identity to send or post vicious or embarrassing material to/about others;
- Denigration -distributing information about another that is derogatory and untrue through posting it on a Web page, sending it to others through email or instant messaging, or posting or sending digitally altered photos of someone;
- Flaming - online "fighting" using electronic messages with angry, vulgar language;
- Blue-jacking - the sending of anonymous text messages over short distances using "Bluetooth" wireless technology;

- Cyber Stalking - repeatedly sending messages that include threats of harm or are highly intimidating, or engaging in other online activities that make a person afraid for his or her safety;
- Outing and Trickery - sharing someone's secrets or embarrassing information, or tricking someone into revealing secrets or embarrassing information and forwarding it to others.

Equal Opportunities / Pupils with additional needs:

- Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety.
- Internet activities are planned and well managed for these children.

Data Protection:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- Data can only be accessed and used on school computers, laptops or authorised encrypted memory sticks. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.
- **Data Protection Act 1998 -** The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

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 Doncaster Local Authority can accept liability for the material accessed, or any consequences of internet access.
- The school should audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

Handling e-safety Complaints:

- All e-Safety complaints must be recorded and passed immediately to the e-Safety Coordinator (see Appendix C).
- 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 safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.

Communication of Policy:

Pupils

- Rules for Internet access will be posted in the ICT suite and all classrooms.
- Pupils will be informed that internet use will be monitored and any inappropriate behaviour will be addressed accordingly.
- The computing curriculum will progressively develop skills and understanding of safe internet use, including strategies for effective and safe research / use of sources online.
- The theme for assemblies will focus on e-Safety and cyber bullying for one half term per year.
- The school will partake in the annual 'Safer Internet Day'.

Staff

- The e-Safety co-ordinator ensures Senior Management and Governors are updated as necessary.
- All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-Safety procedures.
- All staff should be familiar with the school's policy including:
  - safe use of e-mail;
  - safe use of the internet;
  - safe use of the school network, equipment and data;
  - safe use of digital images and digital technologies, such as mobile phones and digital cameras;
  - publication of pupil information/photographs on the school website and virtual learning environment;

  - procedures in the event of misuse of technology by any member of the school community;
  - their role in providing e-Safety education for pupils;
  - reporting procedures for inappropriate material and e-Safety concerns.
- Staff are provided with systematic training about e-Safety, including PREVENT training which is included in the tri yearly safeguarding training schedule. This, in collaboration with in house training, ensures school staff are aware of the dangers and risks associated with the use of technology, including bullying, grooming, the deep dark web, sexting, and radicalisation.
- New staff receive information on the school's acceptable use policy as part of their induction.

Parents

- Parents' attention will be drawn to the school e-Safety Policy in newsletters.
- E-Safety information and up to date links will be added to the school Web site.
- Local Authority support provided to share risks and provide solutions to reduce these.

Community use of the Internet

- Other users using the school's ICT facilities must adhere to the e-Safety policy.

Approved: October 2016

Review: Autumn term 2017

Appendix A

Staff Information Systems Code of Conduct:

To ensure that 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.

- 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/ Designated Safeguarding 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.

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.

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

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

Appendix B

Record of Unsuitable Websites

URL:

Date: **Time**:

Content:

Reported by:

Name: ………………………………………………… Date: ……………………………………
Print name

Signature: ……………………………………………… Designation: ……………………………

Actions Taken:
To be completed by the e-Safety Officer or Computing Co-ordinator

Name: ………………………………………………… Date: ……………………………………
Print name

Signature: ………………………………………………

Appendix C

E-Safety Incident Report

Name of pupil involved: _________________________ Class: ____

Admitted/ Denied (delete as appropriate)

Witnesses: ___________________________________ Class: ____

Description of the incident:
Follow up procedure:

Discussion with pupil	
Support for others involved	
Inform parents (mandatory)	
Inform class teacher	
Inform Headteacher	

Completed by: .... Date: ....
Print name

Signature: .... Designation ....