SHERBURN HUNGATE COMMUNITY PRIMARY SCHOOL

E-Safety Policy

January 2018

<u>E-Safety Policy</u>

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 Pupil Behaviour, Anti-Bullying, Child Protection, Curriculum, Data Protection and Security.

<u>Good Habits</u>

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.

- National Education Network standards and specifications.

<u>Dangers to Consider</u>

Some of the dangers they 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

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

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / 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. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this.

Contents

<u>School e-Safety Policy</u>

The school e-Safety co-ordinator is the Headteacher, Mr Martyn Broom.

Our e-Safety Policy has been written by the school, building on Government guidance. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed in January 2019.

<u>Why is Internet Use Important?</u>

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.

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.

<u>How does Internet Use Benefit Education?</u>

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.

<u>How can Internet Use Enhance Learning?</u>

- 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.

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return the 'Acceptable ICT Use Agreement' which will also be signed by pupils each year.

World Wide Web

- 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.
- 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.

Email and Online Collaboration (Google Drive)

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive messages
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils may must not access others pupil's accounts
- 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 and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted

Social Networking

- Schools should block/filter access to social networking sites and newsgroups 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 should be advised not to place personal photos on any social network space
- 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

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

Filtering

The school will work in partnership with 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 Website

- 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.
- The head teacher or nominee 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 and will not enable individual pupils to be clearly identified on the website
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site
- Work can only be published with the permission of the pupil and parents

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with our technical support team and broadband provider if necessary

<u>Protecting Personal Data</u>

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

<u>Assessing Risks</u>

- 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. The school cannot 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

<u>Communication of Policy</u>

Pupils

- Rules for Internet access will be posted in all networked rooms
- Pupils will be informed that Internet use will be monitored

Staff

- All staff will be given 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

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

Responding to E-Safety Incidents
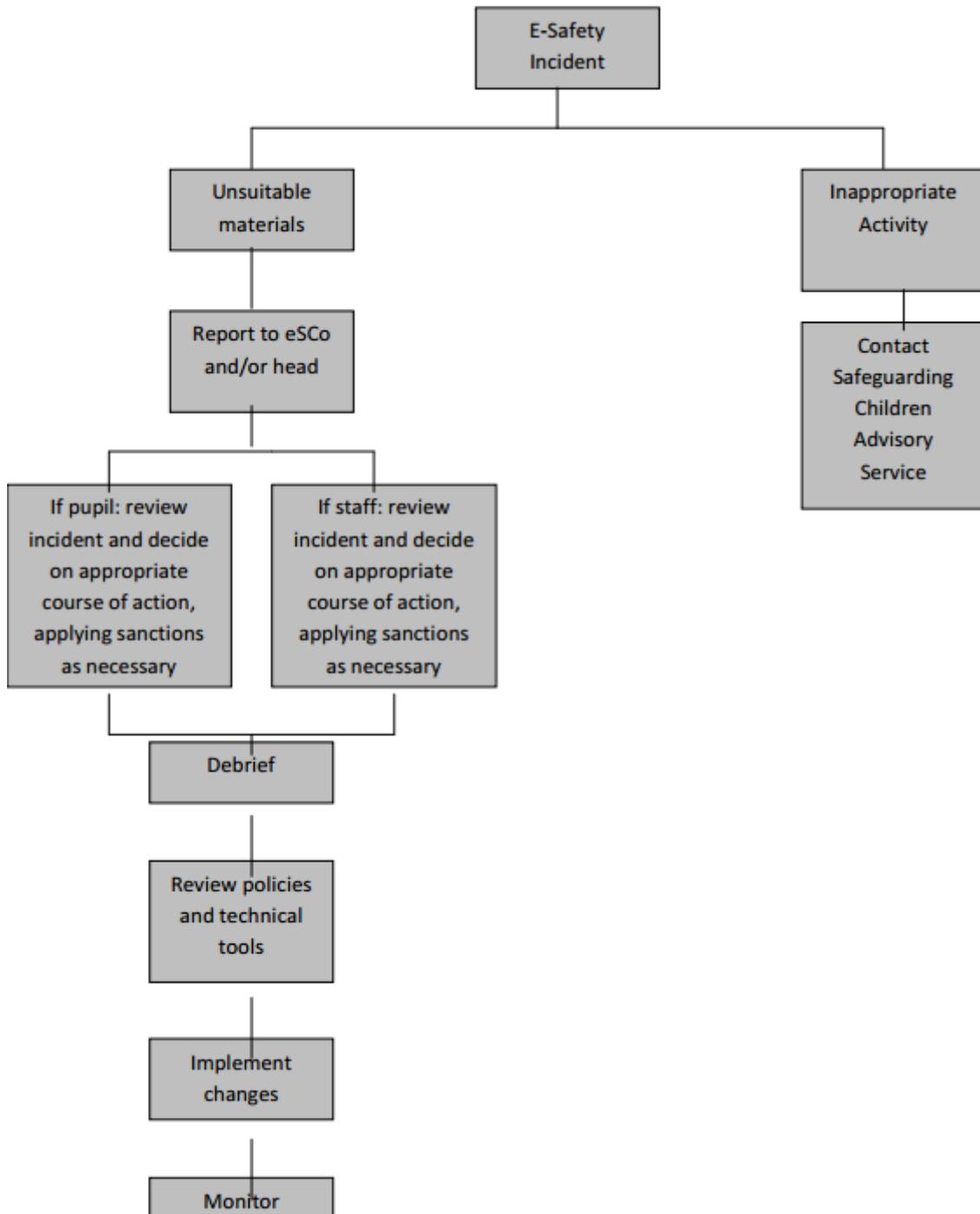
Parent Permission Advice

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:	**Date:**

Please print name:

Please complete, sign and return to the school

Acceptable 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.

YHGfL (Yorkshire & Humberside Grid for Learning) will monitor and audit Internet use to see if users are complying with the policy. Any potential misuse identified by YHGfL 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 web sites, 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 YHGfL:

support@yhgfl.org.uk

- 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 parents will be refused.

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

Signed: …………………………… Capitals: ……………………… Date: ………