eSafeguarding Policy

Ryhill J, I and N School

Est 1913

Together we can achieve

Written by eSafeguarding Co-ordinator – Claire Miller

Reviewed – September 2017

Review date – September 2018

The eSafeguarding policy

The eSafeguarding policy is part of the computing policy and School Development plan with a relation to other policies that include those for behaviour, personal, social and health education and citizenship. The e-Safeguarding Policy and its implementations will be reviewed annually.

The appointed eSafeguarding Coordinators are Claire Miller and Emma Jones
Our eSafeguarding Policy has been written by the school, building on the Wakefield eSafeguarding Policy and government guidance. It has been agreed by senior management and approved by governors.

An overview of the roles and responsibilities of the students, staff Governors and Parent volunteers.

eSafeguarding education will be provided in the following ways:

- A planned eSafeguarding programme will be provided as part of our cyber – bullying information, through SEAL and E-Safety lessons, this will cover both the use of computers and new technologies in school and outside school.

- Key eSafeguarding messages will be addressed through a planned programme of computing and PSHCE lessons.

- Students / pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Students / pupils will be helped to understand the student / pupil AUP.

- Students / pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

- Staff should be aware that they are role models in their use of technologies, the Internet and mobile devices.

Why is Internet use so important?

The rapid developments in electronic communications are having many effects, some profound, on society. Now every pupil is younger than the World Wide Web and many use it more than teachers. Nethertheless it is important to state what we are trying to achieve in education through computing and Internet use.

- 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 schools management functions.

- Internet use is part of the statutory curriculum and a necessary tool for learning.

- Internet access is an entitlement for students who show a responsible and mature approach to its use.

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and the various types of content and to take care of their own safety and security.

How does Internet use benefit education?

The Government set a target that all schools should have broadband Internet use by 2006. Schools should have access to personal learning spaces by 2008 and learning platforms by 2010. Ryhill School has had broadband installed since 2004, personal learning spaces since 2006 and the use of the VLE (learning platform) since 2009.

There are many benefits for the use of a learning platform in school,

- Children will have access to worldwide educational resources including museums and art galleries.

- Inclusion in the National Education Network, which connects all UK schools.

- Educational and cultural exchanges between pupils worldwide.

- Vocational, social and leisure use in libraries, clubs and at home.

- 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.

- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

The school Internet access has been designed expressly for pupils use and includes the filtering systems of; Sophos, Windows defender and a firewall. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. It is planned to enrich and extend learning activities and access levels are reviewed to reflect the curriculum requirements and age of the pupils. Staff give pupils on-line activities that support the learning outcomes planned for the pupil's age and maturity. Throughout school pupils will be educated in the effective use of the Internet and Internet research.

How will e-mail be managed?

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created. Pupils may only use approved e-mail accounts and must immediately tell a teacher if they receive an offensive e-mail. Pupils must not reveal personal details of themselves or other when using e-mail communication. They must never arrange to meet anyone without specific permission. We have the ability to block any external personal e-mail accounts that are inappropriate. E-mails sent to external organisations should be written carefully and authorised by an adult before sending. The forwarding of chain letters is not permitted in school. Staff in school will use either office 360 or their VLE address when dealing with school related issues included emailing each other, as these are filtered and can be monitored.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

How will Internet access be authorised?

The school has allocated Internet access for staff and pupils on the basis of educational need. It is clear who has Internet access and who has not. Parental permission will be required in all cases. The school will maintain a current record of all staff and pupils who are granted access to the schools electronic communications. At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents will be asked to sign and return a consent form for pupil access. Parents will be informed that pupils will be provided with supervised Internet access.

What are the risks of Internet use?

- Receiving inappropriate content
- Grooming
- Requests for personal information
- Viewing "incitement" sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

How will risks be assessed?

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor WDC can accept liability for the material accessed, or any consequences resulting from Internet use. The school audits the technologies used to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

How will eSafeguarding complaints be handled?

Parents, teachers and pupils should make their concerns known to the Headteacher, Computing Co-ordinator, eSafeguarding Co-ordinator or a member of the SLT. Any complaint about staff misuse must be referred to the headteacher and any complaint about the Headteacher must be referred to the Chair of Governors. Prompt action will then occur if a complaint is made and recorded down for reference. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. Other situations could potentially be serious and a range of sanctions will be required, linked to the schools behaviour policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinators (Head teacher or Deputy Head). Advice on dealing with illegal use could be discussed with the local Police Youth Crime Reduction Officer.

How will the policy be introduced to pupils?

As pupils' perceptions of the risks will vary; the eSafeguarding rules will need to be explained or discussed at the start of each school year. There are safety posters with the eSafeguarding rules on which are located around the computer room. This will be discussed with the children, on a regular basis before a computing lesson begins.

Useful eSafeguarding programmes include:

- Think U Know www.thinkuknow.co.uk/
- Grid Club www.gridclub.com
- The BBC Chat Guide www.bbc.co.uk/chatguide/

How will parents' support be enlisted?

Many parents and carers have only a limited understanding of eSafeguarding risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences.

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. Leaflets are given out to the children with eSafeguarding guidance on and what to look out for when their child has access to the Internet. Parents are advised to check if their child's use elsewhere is covered by an appropriate use policy. Parents' attention will be drawn to the school's eSafeguarding Policy in newsletters, the school brochure and on the school website. Internet issues will be handled sensitively, and parents will be advised accordingly. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

An 'Acceptable Use Agreement' will be reviewed annually by the SLT, governors and eSafeguarding Co-Coordinator to be updated. The agreement will then be sent out to parents when their child starts school and is to be signed and returned. Any issues arising will be discussed at that time. This will include where their child's photograph can be displayed e.g. the website, newspapers etc.

Parents will be made aware that videos and still photographs taken by themselves are to be used for personal use only.

Staff training with the eSafeguarding Policy

A planned programme of formal eSafeguarding training will be made available to staff, as part of the safeguarding programme, included extended schools staff,

- All new staff should receive eSafeguarding training as part of their induction programme, ensuring that they fully understand the school eSafeguarding policy and Acceptable Use Policies

- The eSafeguarding policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days/Governors meetings.

- The eSafeguarding Coordinator will provide advice / guidance / training as required to individuals as required

Governor training and the eSafeguarding policy

Governor training will be offered through the attendance at staff INSET days, Governor Services and Bespoke training when available.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their eSafeguarding responsibilities:

The schools IT systems will be managed in ways that ensure the school meets any eSafeguarding technical requirements and any relevant Local Authority eSafeguarding Policy and guidance.

There will be regular reviews and audits of the safety and security of school IT systems. Servers, wireless systems and cabling will be securely located and physical access restricted.

All users will have clearly defined access rights to school IT systems. The Network will record details of the access rights available to groups of users.

The "master/administrator" passwords for the school IT system, used by the Network Manager will also be available for the Head and kept in a secure place

Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that this is known to others.

Any filtering issues should be reported immediately to the LA, who can then subsequently escalate these to the YHGfL support centre.

Requests from staff for sites to be removed or added from the filtered feed will be considered by the Head teacher and if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by Mrs Jones.

Appropriate and relevant security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

Guest and Student accounts are in place with usernames and passwords. These accounts are regularly checked and saved work deleted when no longer in use.

An acceptable use agreement is in place regarding the extent of personal use that users (staff / students / pupils / community users) are allowed on laptops and other portable devices that may be used out of school. These must not be connected to the Internet outside school and only the named user of that laptop is allowed access.

The acceptable use agreement is in place that forbids staff from installing personal programmes on school workstations/portable devices with out the consent from either the Server Manager, Computing Co-ordinator or Head teacher.

The acceptable use agreement is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices. Personal equipment within school is in addition forbidden.

The school infrastructure and individual workstations are protected by up to date virus software.

Personal data cannot be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured.

eSafeguarding and the curriculum

eSafeguarding should be a focus in all areas of the curriculum and staff should reinforce eSafeguarding messages in the use of IT across the curriculum.

- In lessons, processes are in place for dealing with any unsuitable material that is found in Internet searches. These include reporting any misuse to the head teacher and eSafeguarding Co-ordinator.

- Where pupils are allowed to freely search the Internet, staff will be vigilant in monitoring the content of the websites the young people visit.

- Requests for unblocking websites can be made to the YHGfL centre; these requests should be auditable, with clear reasons for the need.

- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

- At the beginning of each school year all children (from FS to year 6) will be asked to sign an 'Acceptable Use Agreement' which will be displayed in their classrooms clearly stating guidelines for the correct usage.