Hollin Primary School
E-safety Policy

OVERVIEW

The focus for this policy is to ensure that existing policies (safeguarding and child protection, behaviour, anti-bullying and Twitter) are applied to the digital environment. In order for this to happen, these policies are regularly reviewed against the Local Authority's and national guidance, and updated as necessary.

OBJECTIVES

- Managing on-line technology so that children are kept as safe as possible.
- Teaching about e-safety/on-line safety
- The responses necessary when a risk to a child is discovered.

Safeguarding children, including e-safety is everyone's responsibility; e-safety is therefore not just the responsibility of just one person, it is a whole school approach.

The overall aims of this policy are to ensure that children:

- Are equipped to access risks in a digital environment (teaching about e-safety)
- Are enabled to make informed judgments about such risk
- Know what to do if something 'not quite right' happens (Zip It, Block It, Flag It)

STRATEGIES

1. Teaching and Learning

Whilst recognising the considerable benefits of new technologies, we teach children to protect themselves from:

- Inappropriate content
- Undesirable contact
- Hurtful conduct

We use the 5 SMART targets. The 'Five **SMART** E-Safety Areas' are as follows:

S – Safe – This gives the children an overview of how to keep safe on the internet, from what information to share online to who you are speaking to. As well as this the children are advised when and where to use personal devices, such as mobile phones and IPADS.

M – Meeting – This makes the children aware that meeting someone online is extremely dangerous and that it should not be done under any circumstances. 'Online Friends Stay Online!'

A – Accepting - This focuses on potential problems that can arise from opening unknown files, E-Mails, Texts, etc.

R – Reliable – This shows the children how easy it is to be misled either on the internet or over the phone, via text. As well as this the children are made aware of the fact that not all the information they find and read online is always true.

T – Tell – This highlights that it is vital to tell somebody, like a friend, teacher, parent and now an E-Safety Ambassador if they have got any issues. We also cover Cyber-Bulling and its effects.

(Incorporating the Zip It, Block It, Flag It slogan)

2. Curriculum Expectations:

Key Stage 1

Pupils should be taught to:

- use technology safely and respectfully,
- keep personal information private,
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2

Pupils should be taught:

- to understand computer networks including the internet;
- how they can provide multiple services, such as the world wide web;
- about the opportunities they offer for communication and collaboration
- how to use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- to use technology safely, respectfully and responsibly;
- to recognise acceptable/unacceptable behaviour;
- to identify a range of ways to report concerns about content and contact.

3. Acceptable Use Policy (AUP)

This sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies. The AUP details how we provide support and guidance to parents /carers for the safe and responsible use of these technologies by adults and children. Each parent/carer signs a contract to ensure that they know what is deemed 'acceptable use of the Internet'.

Appendix 1 – attach a copy of the Parent/Child Agreement

4. Introducing the Policy to Pupils

• Rules for Internet access will be displayed within school. (SMART and Zip It, Block It, Flag It)

• A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and

using online communication appropriately and also the procedure for reporting inappropriate content. (Turn off monitor, tell teacher and report to ICT technician)
• Instruction on responsible and safe use should precede Internet access.
• Pupils will be informed that Internet use will be monitored.
•Children in Key Stage 2 have the expectation to log in on their own individual name and password.
• All Key Stage 1 &2 pupils will be taught about Internet Safety each year and wherever/whenever else is appropriate and necessary.

5. Parents and E-Safety
• Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Website. We will also offer a E-Safety session once a year.
• Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home. This will be done through regular e-safety workshops for parents.
• Internet issues will be handled sensitively to inform parents without undue alarm.
• A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
• All parents will receive support information as and when available.

6. Consulting with Staff and their inclusion in the E-safety Policy
• All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the Internet Access Statement, and its importance explained.
• The school's consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
• All staff must accept the terms of the 'Acceptable Use' statement before using any Internet resource in school.
• Staff should be aware that Internet traffic is monitored and reported by the EDIT and can be traced to the individual user. Discretion and professional conduct is essential.
• The school will adopt the Council's e-mail and Internet user policy.
• The monitoring of Internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
• Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required, but not less than once a year.

WHY WE USE ON-LINE TECHNOLOGY
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
The purpose of using on-line technology 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 business administration systems.

Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

HOW DOES ON-LINE TECHNOLOGY ENHANCE LEARNING?

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Children are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Children are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval.

THE E-SAFETY LEAD

At Hollin Primary School Mrs Geere, who is the designated person for Safeguarding and Child Protection, is also the e-safety lead. The responsibilities of the lead person include:

- Ensuring that policies and procedures include aspects of e-safety
- Working with Edit (Schools IT Company) to ensure that filtering is set at the correct level for staff and children
- Ensuring staff training is provided on e-safety issues each year
- Ensuring that e-safety is included in staff induction
- Ensuring e-safety is covered by children each year
- Monitoring and evaluating incidents that occur to inform future safeguarding and child protection developments

MANAGING SPECIFIC ON-LINE TECHNOLOGIES

1. Internet Access

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form giving permission for their child to use the Internet.

• In Foundation Stage and Key Stage 1, access to the Internet is by adult demonstration and direct supervised access to specific, approved on-line materials.
• In Key Stage 2, pupils will work independently using the internet, but will not be left unsupervised. Pupils are taught the importance of e-safety and agree terms and conditions for acceptable Internet use. Pupils are taught to be critically aware of the materials they read and are made aware that information may be not always be reliable or accurate.

2. The school website:

• The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
• Web site photographs that include pupils will be selected carefully.
• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
• Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

3. Chat and instant messaging

• Pupils will not be allowed access to public or unregulated chat rooms.
• Pupils will not access social networking sites for example 'My Space', 'Facebook', 'Twitter', 'Instagram 'etc
• Any form of bullying or harassment is strictly forbidden.

4. Filtering

• The School works in partnership with parents, Edit and DFE to ensure that systems are in place to protect pupils.
• If staff or children discover unsuitable sites, the URL (address) and content must be reported to Edit via the ICT technician, Mr Hey.
• Any material that the school believes to be illegal must be referred to the Internet Watch Foundation (IWF).

5. Photographic, video and audio technology

• It is not appropriate to use photographic or video devices in changing rooms or toilets.
• Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
• Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities. School equipment should be used for this purpose. Should personal equipment ever be used, then all images must be transferred to school hardware and deleted from the personal device as a matter of urgency.
• Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
• Pupils should always seek the permission of their teacher before making audio or video recordings within school grounds.

6. Mobile Phones

• Children are not encouraged to bring mobile phones in school and are not allowed to use them in school.
• Staff must have their mobile phones on 'silent' during teaching times.
• The sending of abusive or inappropriate text messages is strictly forbidden.

7. Emerging ICT Applications

• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

COMPLAINTS REGARDING THE USE OF ON-LINE TECHNOLOGY

Prompt action is required if a complaint is made. The facts of the case must be established and presented to the e-safety lead/head teacher. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the School's Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Rochdale LEA child protection procedures and our school policy.

Any complaints about staff misuse must be referred directly to the head teacher. Parents and pupils will need to work in partnership with staff to resolve issues. There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

A. How to Respond When a Risk is Discovered

The e-safety lead/head teacher will ensure that the following procedures are adhered to in the event of any misuse of the internet:

1. An inappropriate website is accessed inadvertently:

• Report website to the ICT technician.
• Contact Edit so that the site can be added to the banned or restricted list.
• Change Local Control filters to restrict locally.
• Log the incident.

2. An inappropriate website is accessed deliberately:

• Ensure that no one else can access the material by shutting down the computer.
• Log the incident.
• Report to the head and ICT technician lead immediately.
• Head to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
• Inform the filtering services in order to reassess the filters.

3. An inappropriate website is accessed deliberately by a child:

• Refer the child to the Acceptable use Rules that were agreed.
• Reinforce the knowledge that it is illegal to access certain images and police can be informed.
• Log the incident

• Decide on appropriate sanction.
• Notify the parent / carer.
• Contact the filtering service (Edit) to notify them of the website.

4. An adult receives inappropriate material:
• Do not forward this material to anyone else – doing so could be an illegal activity.
• Alert the ICT technician and head teacher immediately.
• Ensure the device is removed and log the nature of the material.
• Contact relevant authorities for further advice e.g. police, social care CEOP.
• Log the incident.

5. <u>An illegal website is accessed or illegal material is found on a computer</u>.

The following incidents must be reported directly to the police:
• Indecent images of children found. (Images of children whether they are photographs or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
• Incidents of 'grooming' behaviour.
• The sending of obscene materials to a child.
• Criminally racist or anti-religious material
• Violent or bomb-making material
• Software piracy
• The promotion of illegal drug-taking
• Adult material that potentially breaches the obscene publications act in the UK.

6. If any of these are found, the following should occur:
• Alert the ICT technician, Head teacher and E-Safety lead immediately.
• DO NOT LOG OFF the computer but disconnect from the electricity supply.
• Contact the police and or CEOP and social care immediately
• If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer.

7. An adult has communicated with a child or used ICT equipment inappropriately (e-mail/text message etc)
• Ensure the child is reassured and remove them from the situation.
• Report to E-safety lead and Head teacher immediately, who will then follow the Allegations Procedure and Safeguarding and Child Protection Procedures
• Report to the Local Authority Designated Officer.
• Preserve the information received by the child if possible.
• Contact the police as necessary.

8. Threatening or malicious comments are posted to the school website or Twitter page (or printed out) about an adult in school:

• Preserve any evidence and log the incident.
• Inform the Headteacher and E-Safety Lead immediately who will then take any appropriate actions felt necessary.
• Contact the police or CEOP if appropriate.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to head teacher.

9. Threatening or malicious comments are posted to the school website or Twitter pages about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

• Preserve any evidence and log the incident.
• Inform the ICT technician immediately and the E-Safety Lead who will follow the Safeguarding and Child Protection Policy.
• Check the filter if an internet based website issue.
• Contact/parents and carers
• Refer to the bullying policy
• Contact the police or CEOP as necessary.

OUTCOMES

That all staff are aware that safeguarding children, including e-safety is everyone's responsibility; e-safety is therefore not just the responsibility of the Computing coordinator, it is a whole school approach. Staff can manage on-line technology so that children are kept as safe as possible. As a school we respond where necessary when a risk to a child is discovered. Children are equipped to access risks in a digital environment and are able to make informed judgments about such risk. Children know what to do if something 'not quite right' happens (e.g. they are exposed to inappropriate content or undesirable contact)
This policy has been approved and adopted by staff and Governors

Signed …… (Chair of Governors) Date ……

Signed …… (Headteacher) Date ……

Review Date: June 2017