Willerby Carr Lane

Primary School

e-Safety Policy

POLICY MANAGEMENT

Approved by	Full Governing Body
Date approved	25 June 2018
Effective date	26 June 2018
Next review date	Summer 2021
Version Control	The most up to date version of this document is held on the school's intranet

Aims

The school aims to helps pupils to keep themselves safe, including encouraging pupils to adopt safe and responsible practices and deal sensibly with risk, when using the internet.

Objectives

- Children and staff should be able to use the internet and technologies identified within this policy to enhance their teaching and learning.
- Children and staff should be taught a set of safe and responsible behaviours in order to help keep themselves safe on the internet.
- Children and staff should be taught principles of e-safety to help safeguard them both within and outside of school and both now and as they progress to secondary school.
- Parents and carers should be informed of the potential dangers of the internet and its associated technologies and they should be supported by the school to take measures to ensure safe usage by all.

Outstanding provision requires that

1. ALL STAFF share responsibility for e-safety
2. An age appropriate e-safety curriculum helps pupils to stay safe and be responsible users of new technologies
3. The school uses 'Managed systems' rather than 'locked down' ones.
4. Pupils are taught how to manage risk on the internet.
5. There are strong effective links with parents.
6. Good use is made of the views of pupils.
7. There is a systematic review of policy.

Introduction

ICT in the 21st Century is seen as 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, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long 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 and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- 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.

At Willerby Carr Lane Primary School, we understand the responsibility to educate our pupils on eSafety 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.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Responsibilities

Responsibilities of the School Community

We believe that eSafety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team

- Develop and promote an eSafety culture within the school community.
- Support the eSafety coordinator in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafety effectively.
- Take ultimate responsibility for the eSafety of the school community.
- Report any safeguarding children issues in line with the school's Child Protection and safeguarding policy (2017)

Responsibilities of the eSafety Coordinator

- Promote an awareness and commitment to eSafety throughout the school.
- Be the first point of contact in school on all eSafety matters.
- Create and maintain eSafety policies and procedures.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in eSafety issues
- Ensure that eSafety education is embedded across the curriculum.
- Ensure that eSafety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate in line with the school's Child Protection and Safeguarding policy (2017).
- Monitor and report on eSafety issues to the Headteacher as appropriate

Responsibilities of Teachers and Support Staff

- Teach pupils about eSafety in line with the school's eSafety long term plan.
- Read, understand and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy (see appendix).
- Develop and maintain an awareness of current eSafety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed eSafety messages in learning activities where appropriate.
- Report any eSafety-related issues that come to your attention to the eSafety coordinator.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Report any safeguarding children issues in line with the school's Child Protection and safeguarding policy (2017)

Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy (see appendix).
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school ICT system.
- Monitor filtering reports for any eSafety issues.
- Report any eSafety-related issues that come to your attention to the eSafety coordinator.
- Develop and maintain an awareness of current eSafety issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

- Read, understand and adhere to the school pupil Acceptable Use Policy (see appendix).
- Help and support the school in creating eSafety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss eSafety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting eSafety.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss eSafety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's eSafety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the eSafety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety activities.
- Ensure appropriate funding and resources are available for the school to implement their eSafety strategy.
- Ensure policies provide clear guidance relating to the reporting of concerns in line with the school's Child Protection and Safeguarding policy

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide a series of specific eSafety-related lessons in every year group as part of the ICT / PSCHE curriculum.
- We will celebrate and promote eSafety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy (see appendix) which will be displayed in school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this, we will:

- hold parent meetings on eSafety
- include useful links and advice on eSafety regularly in newsletters and on our school website

Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware and will be kept active and up-to-date.
- All users will adhere to an end-user Acceptable Use Policy (see appendix) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- All pupils will access the Internet using an individual log-on, which they will keep secure. Internet access will be supervised by a member of staff.

- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school Acceptable Use Policy (see appendix) at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.
- The school wireless network will be password controlled and the password will be known only by staff so that unauthorised users nearby cannot inadvertently or deliberately connect.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet access

- The school uses a filtered Internet service. The filtering is provided by Smoothwall.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafety coordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, CEOP or IWF.
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning technologies in school

	Pupils	**Volunteers, Students, Parents**	**Staff**
Personal mobile phones brought into school	not allowed	allowed	allowed
Mobile phones used in lessons	not allowed	not allowed	not allowed
Mobile phones used outside of lessons	not allowed	Only allowed away from pupil areas	Only allowed away from pupil areas
Taking photographs or videos on personal equipment	not allowed – except trips	not allowed	allowed with approval from HT

Taking photographs or videos on school devices	Pupils allowed	allowed	allowed
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Pupils not allowed	Not allowed	Staff allowed at certain times (see council IT policy)
Use of personal email addresses in school	Pupils not allowed	Not allowed	Staff allowed at certain times (see council IT policy)
Use of school email address for personal correspondence	Pupils not allowed	Not allowed	Staff allowed at certain times (see council IT policy)
Use of online chat rooms	Allowed within specified application	Allowed within specified application	Allowed within specified application
Use of instant messaging services	Allowed within specified application	Allowed within specified application	Allowed within specified application
Use of blogs, wikis, podcasts or social networking sites	Allowed within specified application	Allowed within specified application	Allowed within specified application
Use of video conferencing or other online video meetings	Allowed within specified application	Allowed within specified application	Allowed within specified application

Using email

- Staff and pupils should use approved e-mail accounts allocated to them by the school and be aware that their use of the school e-mail system will be monitored and checked.
- Pupils will be allocated an individual e-mail account for their use in school.
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender or viewing/opening attachments.
- Pupils are not permitted to access personal e-mail accounts at school.

- Staff may access personal email accounts in line with the restrictions in the Council's IT use policy.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- Images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online.
- Parents, visitors and students are asked not to use their phones while in the school.

Using blogs, wikis, podcasts, social networking and online publishing

We use blogs, wikis, podcasts, social networking within applications specified by teachers to publish content online, to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by pupils will take place within applications specified by the class teacher.
- Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using video conferencing and other online video meetings

We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner:

- All video conferencing activity will be supervised by a suitable member of staff.
- Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.

- Video conferencing equipment will be switched off and secured when not in use.
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off school premises without the permission of the head teacher.

Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Using mobile phones

Children may not bring mobile phones or electronic games onto School Premises or on school trips.

This rule avoids any issues around children disrupting lessons, playing phone games, inappropriate texting and viewing inappropriate pictures or videos. It also avoids the potential loss or accidental damage of expensive items which would result in time consuming investigations.

If any child is found with a phone in school it will be confiscated and the parent rung. Parents will then need to make arrangements for the phones collection from school by a responsible adult of their choice.

Using new technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafety point of view.

We will regularly amend the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafety risk.

Protecting data

We will ensure data is recorded, processed, transferred and made available according to the General Data Protection Regulation 2018. (See GDPR policy)

The school website and other online content published by the school

The school website will not include the personal details, including individual e-mail addresses or full names of staff or pupils.

A generic contact e-mail address will be used for all enquiries received through the school website.

The content of the website will be composed in such a way that individual pupils cannot be clearly identified.

Staff and pupils should not post school-related content on any external website without seeking permission first.

Classifications of eSafety incidents

The following are classified as eSafety incidents:

- accessing illegal content deliberately
- accessing inappropriate content deliberately
- accessing illegal content accidentally and failing to report this
- accessing inappropriate content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school
- accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed
- accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time
- downloading or uploading files where not allowed
- sharing your username and password with others
- accessing school ICT systems with someone else's username and password
- opening, altering, deleting or otherwise accessing files or data belonging to someone else (excluding teachers accessing pupil files)
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature
- attempting to circumvent school filtering, monitoring or other security systems
- sending messages, or creating content, that could bring the school into disrepute
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)

The following are classified as eSafety incidents pertaining to staff:

- transferring personal data insecurely
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)
- failure to abide by copyright of licencing agreements (for instance, using online resources in lessons where permission is not given)

Dealing with E-Safety Incidents

In all cases, report first to the Headteacher who will take any subsequent action. As a guideline the Headteacher may:

- Unsuitable materials (pupil) – review incident; ask parents in to school for meeting, decide on appropriate action which may include exclusion for fixed period.
- Unsuitable materials (staff) – review incident; decide on appropriate action which may include disciplinary action.
- Illegal activity – secure and preserve evidence; report to police.

- Illegal material – secure and preserve evidence; report to police .
- Child or young person at risk –report to police/ ER Safeguarding Children's Board according to the school's Child Protection and Safeguarding policy (2017)

After any incident

- Monitor situation
- Debrief on e-safety incident
- Implement changes
- Review policies and technical tools, and share experience and practice as required

Acceptable Use Agreement: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. The eSafety policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed the school eSafety coordinator.

- ✓ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- ✓ I will not use my own IT equipment/ mobile phones or cameras when working with children unless in agreed by the Headteacher or Deputy.
- ✓ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- ✓ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- ✓ I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- ✓ I will only use the approved, secure email system(s) for any school business.
- ✓ I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- ✓ I will not install any hardware or software without permission of the ICT Technician
- ✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ✓ Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy.
- ✓ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- ✓ I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

Acceptable Use Agreement: Pupils

These rules are designed to keep you safe

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will regularly change my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- ✓ I know that my use of ICT may be denied if I do not comply with these expectation

Smile and Stay Safe Poster

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Toothbrush Poster

Treat your password like your toothbrush… don't let anyone else use it… and change it regularly!

Useful websites

http://www.childnet-int.org/kia/primary/

Childnet's Know IT All for Primary Schools has been especially designed for primary school staff to help them understand important E-safety issues and how to help young pupils get the most out of the internet .

Know IT All for Primary schools also contains a specially designed 5 part 3D animation called 'The Adventures of Kara, Winston and the SMART Crew' This film covers Childnet's 5 SMART rules which have been proven to be effective in helping younger children understand the importance of keeping safe online. Through their travels Kara and Winston use the internet, mobile phones, social networking pages and chat to negotiate and find their way through the adventure. Through their travels they are able to interact with a real life SMART crew of 10 and 11 year old children who give instructions and help Kara and Winston stay safe.

The cartoon will appeal to both younger children (6 and 7) as well as right up to 11 year olds and can be shown in its entirety (15 minutes) or as individual chapters. There are a range of follow up activities and a full lesson plan which you can download.

Smart Adventure Lesson plans have been downloaded to:

- S:\New Shared Area\Curriculum Resources\ICT\e-safety

http://www.thinkuknow.co.uk/

Come in to find the latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it. If you look after young people there's an area for you too – with resources you can use in the classroom, at home or just to get with it. Most importantly, there's also a place which anyone can use to report if they feel uncomfortable or worried about someone they are chatting to online. All the information here is brought to you by the team at the Child Exploitation and Online Protection (CEOP) Centre.

- FS Lee & Kim – cartoon with 5 activities
- KS1 Hector's World – dolphin world cartoon for 5-7 with 5 lesson plans and activities
- KS1 Lee and Kim – cartoon and 7 lesson plans for KS1
- KS2 CyberCafe – cartoon and 9 lesson plans KS2

www.yhgfl.net

A comprehensive eSafety section is available from the YHGfL website

www.saferinternetday.org

Safer Internet Day website