E-Safety Policy

Wheatcroft Primary School & Nursery
Autumn 2018
Review Date: Autumn 2021

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. At Wheatcroft**,** 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.

Aims and objectives

Wheatcroft School aims for all pupils:
In addition to our aims for ICT and Computing, the school aims to:

- Develop all pupils' positive attitude towards e-Safety, and develop an understanding of the appropriate use of technology.
- Provide a safe environment for the use of ICT and teach safe use for all staff and pupils.

Objectives for pupils
Possible teaching and Learning activities see Appendix A.

Learning
The school's internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils using the Hertfordshire Internet and Connectivity Service (HICS). Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience.

Teaching
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

Management and coordination

Information system security
School ICT systems security will be reviewed regularly. The virus protection will be updated regularly and security strategies will be discussed with the Local Authority and ICT technicians. A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. For pupils, reference will also be made to the Behaviour Policy as applicable.

E-mail
In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher or other appropriate adult if they receive offensive e-mail. The forwarding of chain letters is not permitted. Teachers will monitor any e-mails from pupils to external bodies.

Published content and the school web site
Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. Permission must be granted before any material is published.

Pupil's images and work
Images and films of children are stored on our central secure server. Staff should not keep images and/or videos of children on personal laptops. When publishing images, e.g. on the school website, photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs rather than full-face photos of individual children will be used appropriately. High resolution pictures of children will not be used. Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs. Only authorised individuals are able to publish content to our website.

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/carers. This will normally be sought at admission to school and updated in line with privacy guidance.

Social networking and personal publishing
The school will control access to social networking sites, and consider how to educate pupils in their safe use. Pupils will only use moderated social networking sites with supervision and for school purposes. Pupils will be advised to use nicknames and avatars when using social networking sites.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and that age limits (normally 13+) should be adhered to. Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location and that information posted online may be viewed by others, copied and stay online forever. Newsgroups will be blocked unless a specific use is approved.

Managing filtering
The school will work with the Hertfordshire Grid for Learning and Becta to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

Managing videoconferencing & webcam use
Video conferencing should use the educational broadband network to ensure quality of service and security. Pupils must ask permission from the supervising teacher before making or answering a video conference call. Video conferencing and webcam use will be appropriately supervised for the pupils' age.

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. The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones will not normally be used during lessons or formal school time, pupils are not allowed to have mobile phones in School.

The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school. All staff and pupils will agree to its terms and conditions before use and use it appropriately.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulation 2018, including, but not limited to the school giving relevant staff access to its Management Information System, with a unique username and password. Staff are aware of their responsibility when accessing school data and are able to remote access the school server so that no data is stored on any personal device.

Policy Decisions

Authorising Internet access
All staff, governors and visitors must read and sign the Acceptable Use Agreement / Code of Conduct before using any school ICT resource. The school will maintain a current record of all staff, governors, visitors and pupils who are granted access to school ICT systems. Parents will be asked to sign and return the Pupil Acceptable Use Agreement/ e-Safety Rules form for their child/children. (Appendix D)

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Assessing risks
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor HICS can accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints
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. Details of all e-Safety incidents will be recorded by the e-Safety Coordinator using the e-Safety Incident Log. (Appendix E) This incident log will be monitored regularly by the Head teacher, Member of SLT or Chair of Governors.

Communications Policy

Introducing the e-safety policy to pupils
E-Safety rules will be posted in rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and Internet use will be monitored and appropriately followed up. E-Safety lessons are regularly planned as part of the ICT & Computing curricula.
Educating pupils about the online risks that they may encounter outside school is also done informally when opportunities arise, e.g. assemblies or PSHE lessons. Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities. Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying; there is a specific school email for this purpose: safe@wheatcroft.herts.sch.uk. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member.

Staff and the e-Safety policy
All staff will be given the School e-Safety Policy and its importance explained. All members of staff will be asked to sign a Code of Conduct detailing the expectations of acceptable use.

Enlisting parents' and carers' support
Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus, on the school Web site and Learning Platform. The school will maintain a list of e-safety resources for parents/carers. See Appendix C for list of websites for parents.

The school will ask all parents to sign the parent / pupil agreement when they register their child with the school. (Appendix D) This will be updated as necessary.

Resources

Appendix A - Possible teaching and learning activities, with key related e-Safety issues and relevant websites.
Appendix B – List of useful resources for parents.
Appendix C – List of useful resources for teachers.
Appendix D – Acceptable use forms for children, all staff, governors and visitors.
Appendix E – Incident log, to record all e-Safety incidents.

Health and Safety

General health and safety measures are covered in the **Health & Safety Policy** and in the school **Risk Assessment File**.

Schemes of Work

Our school follow the Hertfordshire Computing Scheme of Work, which makes regular reference to e-Safety.

Appendix A – Useful resources for teachers

Bullying
www.bullying.co.uk - One in five young people have experienced bullying by text message or via email. This web site gives advice for children and parents on bullying.

CBBC
http://www.bbc.co.uk/cbbc/topics/stay-safe - The CBBC website has a 'stay safe' area for primary children and has a cartoon and quiz.

Child Exploitation and Online Protection (CEOP) Centre
www.ceop.gov.uk - The Child Exploitation and Online Protection (CEOP) Centre works across the UK and maximises international links to deliver a holistic approach that combines police powers with the dedicated expertise of business sectors, government, specialist charities and other interested organisations - all focused on tackling child sex abuse wherever and whenever it happens. Links to Cyber Café and Hector's World.

Childnet
www.childnet.com **-** *A non-profit making organisation working directly with children, parents and teachers to ensure that the issues of online child protection and children's safe and positive use of the internet are addressed.*

Childnet International produces an online CD guide specifically for parents KnowITAll - http://www.childnet.com/resources/kia/

Children and new technology- the Byronreview
www.dfes.gov.uk/byronreview/ - Safer Children in the Digital World, independent review for the Government looking at the risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games.

Digizen
www.digizen.org/ - in connection with Childnet, this site provides information on cyberbullying and social networking.

European Internet Safety Resource
www.saferinternet.org - Promotes internet safety in Europe with a regular newsletter. Articles on safe use of the internet, mobile phones, gaming, chat rooms by children. Covers what to do about illegal content and harmful content.

Get Safe Online
www.getsafeonline.org - A Government sponsored one-stop-shop for reliable, up-to-date information about online safety, to give home users and small businesses the advice they need to use the Internet safely.

Hertfordshire Police
https://www.herts.police.uk/advice/chatright - internet safety.aspx **-** e-Safety advice from Hertfordshire police, including downloadable materials

Herts Grid for Learning
http://www.thegrid.org.uk/eservices/safety/ - Link to the Hertfordshire Grid for Learning e-Safety advice. Includes powerpoints on e-Safety and lists of useful web pages.

Kidsmart
www.kidsmart.org.uk - Kidsmart is an award winning practical internet safety programme website for schools, young people, parents, and agencies, produced by the children's internet charity Childnet International.

London Grid for Learning
http://www.lgfl.net/esafety/Pages/safeguarding.aspx - Resources, web links and downloadables aimed at school staff.

Teachers TV
https://www.tes.com/teaching-resource/teachers-tv-ks3-4-ict--online-safety-6039010
This programme outlines simple classroom activities to help teachers to take practical steps to keep pupils safe online and to increase awareness of the potential dangers of internet usage.

Thinkuknow
www.thinkuknow.co.uk - The Child Exploitation and Online Protection (CEOP) Centre has website which has been designed and written specifically for children of different ages to ensure children stay safe on the Internet. It also has sections specifically developed for parents/carers and teachers/trainers.

Appendix B – Useful resources for parents

BBC Chatguide
http://www.bbc.co.uk/webwise/topics/safety-and-privacy/ - part of the BBC guidance to support parents with information relating to internet safety.

Bullying
www.bullying.co.uk - One in five young people have experienced bullying by text message or via email. This web site gives advice for children and parents on bullying.

CBBC
http://www.bbc.co.uk/cbbc/topics/stay-safe - The CBBC website has a 'stay safe' area for primary children and has a cartoon and quiz.

CEOP
http://ceop.police.uk/safety-centre/ **-** The National Crime Agency's online centre for e-Safety advice, featuring a reporting mechanism to alter authorities regarding inappropriate conduct towards a child online.

Chat Danger
www.chatdanger.com - Childnet have developed this interactive to provide children and young people with information, advice, true stories, safety tips and a quiz site all about the potential dangers on interactive services online like chat, IM, online games, email and on mobiles.

Childnet
www.childnet.com **-** *A non-profit making organisation working directly with children, parents and teachers to ensure that the issues of online child protection and children's safe and positive use of the internet are addressed.*
Childnet International produces an online CD guide specifically for parents KnowITAll - http://www.childnet.com/resources/kia/

Get Safe on Line
www.getsafeonline.org - A government sponsored one-stop-shop for reliable, up-to-date information about online safety, to give home users and small businesses the advice they need to use the Internet safely.

Hertfordshire Police
https://www.herts.police.uk/advice/chatright - internet safety.aspx **-** e-Safety advice from Hertfordshire police, including downloadable materials

Herts Grid for Learning.
http://www.thegrid.org.uk/eservices/safety/index.shtml - e-Safety advice for schools, includes list of useful web pages.

http://www.thegrid.org.uk/eservices/safety/parents.shtml - e-Safety advice for parents, includes list of useful web pages.

Kidsmart
www.kidsmart.org.uk/ - Kidsmart is an award winning practical internet safety programme website for schools, young people, parents, and agencies, produced by the children's internet charity Childnet International.

Microsoft e-Safety advice
http://www.microsoft.com/security/default.aspx - Advice from Microsoft about staying safe online, password protection and avoiding scams. Aimed at adults.

Safer Internet
www.saferinternet.org.uk - The UK Safer Internet Centre is coordinated by a partnership of three leading organisations; Childnet International, the South West Grid for Learning and the Internet Watch Foundation. Features advice and research.

Thinkuknow
www.thinkuknow.co.uk - The Child Exploitation and Online Protection (CEOP) Centre has a website which has been designed and written specifically for different ages of children to ensure children stay safe on the Internet. There is also a section for parents offering advice and support.

Appendix C – Acceptable Use Forms

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This 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 with Mrs Miller or Miss Brown.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- 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, personal e-mail address, personal social media account, or any other link to pupils.
- I will not wear a SmartWatch in any public area of the school premises
- I will ensure that personal cameras or mobile phones will not be kept in teaching spaces.
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) 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 Headteacher or governing body.
- I will not install any hardware or software without permission of the Headteacher or reference to the ICT Technician[s].
- 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 using school digital cameras and not personal mobile phones or cameras; stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I will follow requirements for data protection as outlined in GDPR policy. These include: Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not access secure school information from personal devices unless a closed, monitorable system has been set up by the school.
- I will ensure that personal or sensitive data taken off site must be encrypted.
- I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parent/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.
- My private account position will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.
- I will not upload any materials about or reference to the school or its community on my personal social networks.
- I will pre-check for appropriateness all internet sites used in the class: this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of pupils. If unsure I will seek approval from the Head before I use it.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……(printed) Job title……

Pupil Acceptable Use Agreement / eSafety Rules

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Miller or Miss Brown.

- ✓ I will only use school IT equipment for activities agreed by school staff.
- ✓ I will not use my personal email address or other personal accounts in school when doing school work.
- ✓ I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- ✓ I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- ✓ In school I will only open or delete my files when told by a member of staff.
- ✓ I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- ✓ I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- ✓ If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- ✓ If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- ✓ I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- ✓ Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- ✓ Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- ✓ I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- ✓ I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- ✓ I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- ✓ I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- ✓ I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

✂ -

Parent/ carer & child signature

We have discussed this and …………………………………………...(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Wheatcroft Primary School.

Child Signature …………………………………………………………Parent/ Carer Signature …………………………………………………….

Class …………………………………… Date ……………………………….

Appendix D – Incident Log

Wheatcroft Primary eSafety Incident Log

Details of ALL eSafety incidents to be recorded. This incident log will be monitored regularly by the e-Safety Coordinator, Headteacher, Member of SLT or Chair of Governors.

Date & time	Name of pupil or staff member	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons