White Spire School

E-Safety Policy

Department:	ICT
Author:	P Wilson
Next Review date:	October 2019

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband managed in school;
- A school network that complies with the National Education Network standards and specifications.

1.0 In conjunction with:
Milton Keynes Council
Children and Young People's Services Directorate

School e-safety policy

2.1.1 Writing and reviewing the e-safety policy
The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- Our e-Safety Coordinator is P Wilson, the role is done in conjunction with the Designated Child Protection Coordinator.
- Our e-Safety Policy has been written by the school, using guidance from the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The policy is shared with all teaching staff including TAs and HLTAs within a staff meeting.
- The e-Safety Policy was revised by: P Wilson
- It was approved by the Governors – 09.11.2017
- The next review date is (at least annually): October 2019
- The e-Safety policy should be read in conjunction with the school Child Protection Policy for guidance on Prevent, Child Sexual Exploitation, etc.

2.1.2 Safeguarding
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material ; for example pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

This policy and the procedures within are in place to ensure pupils and staff are protected from harm to the highest extend practicable.

2.2 Teaching and learning

2.2.1 Why the Internet and digital communications are important

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

2.2.3 Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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.

2.2.4 Pupils will be taught how to evaluate Internet content

- 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.
- Pupils will be taught how to report unpleasant Internet content by reporting to a member of staff or parent who will take the necessary action.

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT systems security is reviewed regularly by the IT Systems Manager.
- Virus protection is updated automatically by the provider, ESET, and is at least once daily.
- Security strategies will be discussed with the Local Authority when requested.

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive 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.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupils are taught how e-mail from and to external bodies is presented and controlled.

- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school web site

- Staff or pupil personal contact information is not published. The contact details given online are the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- School keeps a list of pupils whose image is not permitted to be used for any purpose including Internet publications

2.3.5 Social networking and personal publishing

- The school controls access to social networking sites, and educates pupils in their safe use through the teaching of e-safety in ICT lessons.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils would use only moderated social networking sites, e.g. SuperClubs Plus
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for special needs pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff should not be using social networking sites in school.
- Staff should not add existing pupils on social networking sites.

2.3.6 Managing filtering

- Filtering is managed through Opendium's Web Gateway product.
- The DNS services that we use are an internal DNS called PiHole an then re-filter through OpenDNS Service which is a further level of school specific filtering.
- E-mail is outsourced to Google who do heavy duty checking on incoming/outgoing email.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing & webcam use

- Pupils do not yet use videoconferencing but should it be used in the future it will use an education specific provider such as vidyo.com to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

2.3.8 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 be used during lessons or formal school time, pupils are told to hand in phones at the beginning of the day and to collect them on the way home. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones is not permitted.
- Games machines, for example in After School Club, are not connected to the Internet as their use may not include filtering.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils. All staff have access to cameras to take photographs.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulation 2018.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read and sign the "Staff Code of Conduct for ICT" before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- Parents and pupils are asked to sign and return a consent form as part of the home/school agreement.

2.4.2 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 Milton Keynes Council 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.

2.4.3 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.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

2.4.4 Community use of the Internet

- If the need arises the school will liaise with local organisations to establish a common approach to e-safety.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all 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.
- A programme of training in e-Safety is in place and is based on the materials from CEOP.
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHCE) curriculum.

2.5.2 Staff and the e-Safety policy

- All staff are given the School e-Safety Policy and its importance explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be managed by senior management and work to clear procedures for reporting issues.

- Staff and pupils use Google search with "Safe Search" (a Google feature) is enforced and HTTPS inspection takes place to stop encryption being used to hide search results.

2.5.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Appendix 1: Quick Guide to E-Safety in School

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Learning Zone The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	SuperClubs Plus School Provided Account Kids Safe Mail Kent Learning Zone Cluster Microsite blogs
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on "moderated sites" and by the school administrator.	Making the News SuperClubs Plus Headline History Kent Grid for Learning Cluster Microsites National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

BBC Stay Safe

www.bbc.co.uk/cbbc/shows/stay-safe

General Internet safety site

www.childnet.com

Child Exploitation and Online Protection Centre

www.ceop.gov.uk/

Digizen – responsible digital citizen

www.digizen.org/

Kent Police – e-Safety

https://www.kent.police.uk/advice/online-safety/how-to-protect-your-digital-identity/

Think U Know

www.thinkuknow.co.uk/

Safer Children in the Digital World

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Appendix 3: Useful resources for parents

Care for the family

Family Online Safe Institute

www.fosi.org

Internet Watch Foundation

www.iwf.org.uk

Appendix 4: Designated Leads

Finlay Douglas – Headteacher – Deputy Designated Safeguarding Lead

Michelle Bartle – Assistant Head – Senior Designated Safeguarding Lead

Phil Wilson – Assistant Head – Designated Safeguarding Lead

Katy Cozens – Assistant Head - Designated Safeguarding Lead

Shams Sharples – Primary Lead - Designated Safeguarding Lead

Sophie Lunnon – Behaviour Support - Designated Safeguarding Lead

Debora Robinson - HLTA - Designated Safeguarding Lead

Sally Seminario - Office - Designated Safeguarding Lead

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail and social networking, and that ICT use may also include personal ICT devices when used for school business
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher
- I understand that my use of school information systems, Internet and e-mail may be monitored and recorded to ensure policy compliance
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager
- I will not install any software or hardware without permission
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely
- I will respect copyright and intellectual property rights
- I will report any incidents of concern regarding children's safety to the head teacher (e-Safety Coordinator and Designated Child Protection Coordinator)
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing
- Student data not to be taken off site unless authorised by the Headteacher

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and do accept the Staff Code of Conduct for ICT.

Signed: **Capitals:** **Date:**

Accepted for White Spire School

Visitor Code of Conduct for ICT

To ensure that visitors are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Visitors should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail and social networking, and that ICT use may also include personal ICT devices when used for school business
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher
- I understand that my use of school information systems, Internet and e-mail may be monitored and recorded to ensure policy compliance
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager
- I will not install any software or hardware without permission
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely
- I will respect copyright and intellectual property rights
- I will report any incidents of concern regarding children's safety to the head teacher (e-Safety Coordinator and Designated Child Protection Coordinator)
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing
- Student data not to be taken off site unless authorised by the Headteacher

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and do accept the Visitor Code of Conduct for ICT.

Signed: **Capitals:** **Date:**

Accepted for White Spire School