Wheatlands Primary School
E-Safety Policy

Our Vision

Wheatlands Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, we aim to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people whilst on the school premises.

Writing and reviewing the E-Safety Policy

The E-Safety Policy relates to other policies on safeguarding including those for ICT, bullying and for child protection. The school has appointed Mrs Claire O'Malley to the role of E-Safety Officer who will work closely with the designated Child Protection person as the roles may overlap. It is not a technical role.

Our E-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.

- The E-Safety Policy was revised by Mrs O'Malley
- The next review date is September 2020

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing E-Safety issues at our school. Mrs O'Malley is the central point of contact for all E-Safety issues and will be responsible for day to day management. All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the E-Safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

Teaching and Learning

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 and to help them learn about the benefits, risks and dangers of the internet. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils and access to safe search facilities as appropriate.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Access for staff may be at a different level to pupils.
- 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. 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 how to report unpleasant Internet content.

Children in all classes in school will have access to the internet. However some different types of use are outlined below:

- Online content (e.g., CBeebies) will often be used by the teachers for specific tasks. In these situations the children are not searching the internet or navigating away from the page/s and tasks that have been set. Teachers will have previewed the site to ensure that it matches the learning outcomes of the lesson/setting. With younger children it is essential that access to navigate away accidentally is denied (i.e., hiding the address bar)
- Searchable cached sites such as Espresso will allow access within a site but not beyond it
- When considered appropriate children may use a safe search engine when searching for information. This is not a failsafe way of preventing access to inappropriate sites but is a good line of defence. Searches will only be permitted when a member of staff if present. Where possible teachers should have pre-searched for the topic in hand and previewed the hits that will be used based on the fact that search engines do not necessarily give the most appropriate site at the top of their lists
- In most cases key websites will be identified by the teacher for the children to use to find information.

<u>Managing Internet Access</u>

Information system security

- School ICT systems security will be reviewed regularly and improved.
- Virus protection will be updated regularly.
- Security strategies will be discussed with OneIT
- E-mail – all staff have ‘professional’ e-mail accounts. Children will be provided with e- mail accounts when appropriate e.g. for a specific project.
- School or work e-mail addresses are not used for personal private use.
- Staff and pupils may only use approved e-mail accounts on the school system.
- Staff and pupils must report 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 and attachments should be treated with care.

Reporting Accidental Access to Inappropriate Material

Like any online service, it is impossible to guarantee that there will never be accidental access to inappropriate or offensive material. Any user of the school's network who accidentally comes across inappropriate or offensive material should do the following:

1. Inform the school's E-Safety officer of the incident and give the website address.
2. Ask the E-Safety officer to log the web address, time and username using an e-safety incident report form (see page 7)
3. The school's E-Safety officer should contact the Trust's representative.

The outcome of the investigation will be relayed back to the Trust's representative. If it is decided that the website is not sufficiently inappropriate for global blocking, the school will need to make a localised decision to block the website via the school's filtering solution provided by OneIT.

Reporting Suspected Deliberate Abuse or Misuse

Any person suspecting another of deliberate misuse or abuse of the broadband network should take the following action:

1. Report in confidence to the school E-Safety officer or Headteacher of the school.
2. The Headteacher should inform the Trust.
3. The Trust should complete an internal investigation form.
4. If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, the Trust will inform the relevant police authority who will complete their own investigations.
5. If the investigation confirms that inappropriate behaviour has occurred, the Trust will inform the relevant authority. This may be the Local Authority or the School's Board of Governors.
6. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Examples of Inappropriate Use:

- Visiting pornographic sites (adult top shelf materials)
- Causing offence to religious groups
- Inappropriate use of e-mail
- Deliberate sabotage of the network; i.e. hacking, mail bombing, etc.
- Violence
- Racism
- Illegal drug taking and promotion of illegal drugs
- Criminal skills, proxy avoidance and software piracy.

Access to Illegal Material

If this investigation results in confirmation of access or attempted access to illegal materials or the committing of illegal acts, the Trust will inform the relevant police authority that will complete their own investigations and a criminal investigation may follow. Examples of Illegal Acts:

- Accessing any child abuse images.
- Incitement to racial hatred
- Incitement to violence
- Software media counterfeiting or illegitimate distribution of copied software.
- Accessing extreme pornography

More information is available at http://www.govconnect.gov.uk/

Decision to Advise the Police for Criminal Investigation

On the facts that are immediately available, a decision will be taken whether to refer the matter to the Police for criminal investigation. This does not preclude the matter being referred to the Police at any later stage when a formal investigation has been undertaken.

Published content and the school website

- Staff personal contact information will not generally be published. The contact details given online will be the school office. It is good practice to create an admin account for this.
- Pupil personal contact information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Staff will consider using group photographs rather than full faced photos of individual children.
- Pupils' full names will not be used anywhere on a school website 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, prospectus or other forms of media.
- Work can only be published with the permission of the pupil and parents/carers. Pupil image files will not refer to the pupil by name.

Social networking and personal publishing

- The school will control access to social networking site and consider how to educate pupils in the safe use of social networking sites. .
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Staff and parents will be advised that the use of social network spaces outside school brings a range of dangers. Parents of upper key stage two children will be invited into school to work with an outside agency to provide support and guidance on the use of these sites.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff should follow professional guidance and not have children as friends on social networking sites.
- Where issues arise with members of staff and pupils who are related to them, staff should exercise caution, professional judgement and use privacy settings to ensure all communications are appropriate.

Managing Filtering

The schools internet is provide through OneIT using education firewalls, in addition to each school having its own local firewall to protect the curriculum network. All Internet traffic is monitored and filtered through a centralised Smoothwall filtering system. This is in line with the Byron report (2008).

- Schools should not use any other filtering system without the express permission of their Head teacher.
- Schools are permitted to request websites to be unblocked through Smoothwall, but should only do so if newly allowed websites have been checked by the school's e-safety officer.
- Schools must request websites to be blocked/unblocked by asking OneIT.

- The school will work with OneIT 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 Officer.

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 without prior agreement with the Headteacher. 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 will be kept under review.
• Games machines including the Nintendo Wii, Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
• Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times. It is forbidden to use these for personal use.

• To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
• Staff understand that they should use their own mobile phones sensibly and in line with school policy. Personal mobile phones must not be used to take photos of pupils.

Use of Mobile Devices whether Owned by Schools or Individuals

It is strongly recommended that mobile devices access the Internet via the filtering provided by OneIT as described above. However, users should note the following items. These examples are for clarification. They are not exclusive:
• Any mobile device must be checked for viruses and spam content before being attached to the regional broadband network.
• Mobile devices must not be used to take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission.
• Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.

It is advisable for staff to have a passcode on their personal mobile phones. If staff have their school e-mail account linked to their phones, then staff must have a passcode.

Protecting personal data - Data Handling and Data Transfer

Personal data will be recorded, processed, transferred and made available according to GDPR. Requirements are being developed for protecting data when transmitted across a broadband network or the Internet. Good practice dictates that all data which refers to individuals or contains sensitive information of any kind should be encrypted.

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

- Parents will be asked to sign and return an AUP.
- Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

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 the Trust can accept liability for any material accessed, or any consequences of Internet access.

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

Communications Policy

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.
- E-Safety training will be embedded within the ICT scheme of work.

Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school Website.

E-Safety Incident Reporting Form	
Date of Incident:	
Member of staff reporting the incident:	
Web address of the incident:	
Copy of screens or other evidence saved to/filed in:	
Location of incident:	
Computer serial number:	
Details:	
Action taken:	
Reported to:	