Wheelock Primary School

Online Safety Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites, including the school website.
- Email and instant messaging apps.
- Social networking
- Blogs and wikis
- Podcasting and video calling
- Music downloading
- Gaming, including chatting online.
- Mobile phones texting/WhatsApp/video function
- Zoom
- Live Streaming
- Artificial Intelligence

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. Some of the dangers they may face include:

- Access to illegal, harmful, or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- Sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication with others, including strangers.
- Cyberbullying
- An inability to evaluate the quality, accuracy, and relevance of information online, including the phenomena of 'fake news.'
- Plagiarism and copyright infringement
- Downloading content illegally
- The potential for excessive use which may impact on the child's social and emotional development and learning.

At Wheelock Primary School we understand the responsibility to educate our pupils on Online Safety 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 Policy (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, netbooks, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones).

Scope of the Policy

This policy applies to all members of the academy community who have access to and are users of ICT systems, both in and out of the building.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of the school. Wheelock Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate e-safety behaviour.

Homophobic, BI phobic and transphobic language and online bullying both on school computers and outside of school will not be tolerated and the same sanctions will apply as in the classroom.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole community. It is linked to the following mandatory policies: child protection and safeguarding, acceptable use, cameras and mobile phones, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy, CCTV and PHSE.

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership at Wheelock Primary School, the principal and Local Advisory Board have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety Officer in our school is Sally Whitehead supported by Stuart Owen who is the computing lead within the school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Senior management and governors are updated by the principal / Online Safety Officer.

Principal and Senior Leaders

- The principal is responsible for ensuring the safety (including online safety) of members of the academy community.
- The Principal is currently the designated online safety officer.
- The principal is responsible for ensuring that staff receive suitable CPD to enable them to conduct their online safety roles.
- The principal will ensure that there is a system in place to allow for monitoring and support of those in the academy who conduct the internal online safety monitoring role.
- The principal is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Officer

Ensures that all staff are aware of the procedures that need to be followed in the event of a digital safety incident taking place.

- Provides training and advice for staff.
- Liaises with other agencies.
- Liaises with the Computing Coordinator.
- Receives reports of online safety incidents.
- Attends relevant Governor Board meetings.
- Keeps up to date with current issues and guidance through organisations such as SCIES, CEOP (Child Exploitation and Online Protection), NSPCC, Childnet and Internet Safety Matters.

The ICT Technicians

The ICT Technicians are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements.
- That users may only access the academy's networks through a properly enforced password protection policy.
- That the school uses the Talk Straight filtering service.
- That any misuse / attempted misuse of the network or email is reported to the Digital Safety Coordinator.

The Computing Subject Leader

The Computing Subject Leader is responsible for ensuring:

- The curriculum teaches online safety appropriately.
- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the online safety technical requirements.
- That users may only access the school's networks through a properly enforced password protection policy.
- That any misuse / attempted misuse of the network / Virtual Learning Environment (VLE) / email is reported to the Online Safety Coordinator.

Staff

- New staff receive information on the academy's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know to report the misuse of technology by any member of the academy community to the Online Safety Officer.
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.
- Teaching and support staff are responsible for ensuring that:
    - Digital communications with pupils should be on a professional level.
    - They monitor computing activity in lessons and extracurricular activities.
    - They are aware of esafety issues related to the use of all electronic devices.

Designated Person for Child Protection and Safeguarding

The designated person for child protection and safeguarding is trained in online safety issues and is aware of the potential for serious child protection issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

Pupils

- Are responsible for using the ICT systems in accordance with the Acceptable Use Policy, which they (or their parents/carers) will be expected to sign before being given access to systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Parents/Carers

Parents and carers will be responsible for:

- Endorsing the Acceptable Use Policy
- Parents and carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on the school website, newsletter, and social media).
- Children and their Parents/Carers have received a home school agreement regarding acceptable use of IT in school.
- Parent/carers have access to material sent out by school to update them on current safety issues for online safety as receive guidance on how to support at home.

Embedding E Safety Messages across the school

- We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.
- Pupils will be informed that Internet use will be monitored in acceptable use policy.
- All staff will be given the Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic is monitored and traced to the individual user on any school device at school and off the premises. Discretion and professional conduct is essential.
- Parents' attention will be drawn to the Online Safety Policy in newsletters and on the website.

Continuing Professional Development

- Training will be offered as follows:
- All new staff should receive Online safety training as part of their induction programme, ensuring that they fully understand the online safety policy and Acceptable Use Policies
- The Online Safety Officer will receive regular updates through training sessions and by reviewing guidance documents.
- This Online Safety policy and its updates will be presented to staff.

Training for Local Governing Body

Governors should take part in Online safety awareness sessions. This may be offered through participation in training or through specific information sessions.

Equipment, filtering, and monitoring

Filtering

The Academy will work in partnership with other agencies to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

Emerging technologies will be examined by Computing Subject Leader for educational benefit, and a risk assessment will be carried out before use in the academy is allowed.

Information System Security

- ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the ICT Technician

Equipment

- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- The "administrator" passwords for the ICT system, used by Novus only.
- Executable files can only be run using the "administrator" rights.
- See iPad and laptop policy for information about devices which are taken off the premises.
- The network and individual workstations are protected by up-to-date virus software.

Monitoring

- There will be regular reviews and audits of the safety and security of ICT systems.

Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum, and we continually look for new opportunities to promote Online Safety. Please see Computing curriculum overview.

Online Safety education will be provided in the following ways:

- The school follows the curriculum 2014 requirements. They use National Online Safety and Purple Mash platforms to teach children about Online Safety.
- Educating all pupils on the dangers of technologies that maybe encountered outside school is done formally as part of the computing curriculum.
- Pupils are 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, or an organisation such as Childline/ CEOP report abuse button.
- Online messages are reinforced in assemblies.
- Junior Safety Officers support all the children and staff in school to understand Online Safety and how to stay safe online for example they support the participation of Safer Internet Day.
- Pupils are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices

both within and outside the academy.

- Where pupils are allowed to freely search the internet, e.g., using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination).

Equal Opportunities

Wheelock Primary School endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of our Online Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Managing the Internet
Use of the Internet to Enhance Learning

- The academy internet access is designed for pupil use and includes filtering.
- Pupils are taught what internet use is acceptable and what is not.
- Internet access will be planned to enrich and extend learning activities.
- Staff will preview any recommended sites before use.
- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval, and evaluation.

Authorised Internet Access

- All staff must read and sign the 'Acceptable Use Policy' before using any academy ICT resource.

Internet

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the support technician via the principal.
- The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- It is the responsibility of the academy, by delegation to the ICT technician, to ensure that anti-virus protection is installed and kept up to date on all academy machines.

Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of Wheelock Primary School, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be the staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'etiquette.'

- The school gives all staff their own email account to use for all academy business. This is to minimise

the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary. email histories can be traced. This should be the account that is used for all academy business.
- Email should not be displayed on Interactive Whiteboards.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses or phone numbers. Staff use 'no caller ID' to make calls to families from their personal phones.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or to arrange to meet anyone without specific permission.
- Access in the school to external personal e-mail accounts may be blocked.

Social Networking

Personal use of public social networking sites (e.g., Twitter, Facebook, Instagram) is not allowed in school. Members of staff with access to the school Facebook account may use the school account.

The academy will block/filter access to social networking sites unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are taught not to place personal photos on any social network space.
- The curriculum, through Purple Mash, supports the understanding of the dangers of these platforms and how to keep themselves safe online.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018. The key principles are:

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged out" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick, or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer.

- The academy will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

- Currently pupils are not allowed to use personal mobile devices/phones in school. KS2 children, who may be walking home alone, carry a mobile phone but this must be stored with the class teacher during the school day, and children are not allowed to have access to them. This is at parents' own risk.

- The school is not responsible for the loss, damage, or theft of any personal mobile device.

- The sending of inappropriate text messages between any members of the school community is not allowed.

Responding to incidents of misuse

If any apparent or actual misuse appears to involve illegal activity contact the safeguarding lead immediately i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity, or materials

Pupils are encouraged to inform their teacher or other adults in the school regarding anything which makes them feel uncomfortable while using ICT.

- Complaints of Internet misuse will be dealt with by the principal and recorded on CPOMS
- Any complaint about staff misuse must be referred to the principal.
- Complaints of a child protection nature must be reported to the Named Persons for Child Protection – Sally Whitehead

Monitoring and Review Process

The implementation of this policy will be monitored annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken

place.