WIDDEN PRIMARY SCHOOL

e-SAFETY POLICY

REVIEWED BY:

Rachel Kittle

DATE APPROVED BY THE FULL GOVERNING BODY:

7th March 2023

REVIEW CYCLE

Annually

NEXT REVIEW DUE:

February 2024

Policy Statement

At Widden Primary School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to entrust the whole school community with the ability to stay safe and risk free.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce the potential of harm to the pupil or liability to the school.

This policy is available for anybody to read on the Widden Primary School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Acceptable Use Policy. A copy of the Pupils' e-Safety agreement will be sent home with pupils at the beginning of each school year with parents required to sign. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Introduction

Information Technology (IT) and Computing in the 21st Century are seen as an essential resources to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Schools need to build in the use of these technologies in order to enable our young people with the skills to access life-long learning and future employment.

At Widden Primary School we understand the responsibility to educate our pupils on e-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, whilst in and beyond the classroom.

Both this policy and the Acceptable Use Policy and Agreement (for all staff, governors, visitors and pupils) are inclusive of:

- Fixed Internet (LAN and WiFi).
- Mobile Internet (including staff personal use of mobile phones when on site)
- Technologies provided by the school (such as PCs, laptops, tablets and interactive whiteboards/TVs)

Policy Governance (Roles & Responsibilities)

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored and that school filtering and monitoring systems are regularly reviewed. The DSL and Computing Lead, alongside the teaching staff, are to ensure the safety of pupils online is monitored and any issues arising will be to notify the Head immediately.

This policy, supported by the school's Acceptable Use policy and Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, and behaviour (including the anti-bullying) policy**.**

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- The school has a duty to provide students with quality Internet access as part of their learning experience
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security

How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the LA (Local Authority) and DfE (Department for Education)
- Access to learning wherever and whenever convenient

How can the Internet enhance learning?

- The School Internet access is designed for pupil use and includes filtering appropriate to the age of pupils
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the 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 evaluated.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Site Manager in the first instance and then communicated to the Computing lead.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law

- Pupils should be taught to be aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of on-line materials is a part of every subject

How will ICT system security be maintained?

- The security of the school ICT systems will be reviewed regularly
- Virus and ransomware protection will be installed and updated regularly
- Personal data sent over the Internet will be encrypted or otherwise secured
- Use of portable media will be reviewed. Portable media may not be used without specific permission and a virus check
- Files held on the school's network will be regularly checked
- The dedicated IT technician will review system capacity regularly
- Staff are encouraged to make use of the 'One Drive' facility for storage within their Office 365 package.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone
- Whole-class or group e-mail addresses can be created for pupils use when learning about emails and will need to be setup by the IT technician or computing lead.
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to an external organisation should be carried out professionally and checked for accuracy before sending, in the same way as a letter written on school headed paper

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting
- The Headteacher, along with the support of staff with designated admin rights, will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright

Can pupil's images or work be published?

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs

- Permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupils learning outcomes may be shared online and celebrated on year group blogs.

How will social networking and personal publishing be managed?

- Pupils are advised never to give out personal details of any kind, which may identify them or their location. Examples would include real name, address, contact phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. House number, street name, school, shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others
- Pupils should be advised not to publish specific and detailed private thoughts
- We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments
- The school's PSHE scheme of work has been extended to incorporate the education of children on the Internet and its safe use
- During school events where parents are invited in or to attend, staff are to remind and advise parents not to publish any content of images/ videos on any social media platform without prior consent of the parent of the child.

How will filtering be managed?

- Internet Filtering is provided by RM Unify.
- We will work in partnership with parents, the LA, DfE and our ICT support provider, EntrustFocus Networks, to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the DSL in the first instance and then communicated to the Computing lead. Children will be educated as to the correct and safe procedure to do this
- Any material that the school believes is illegal must be referred to the Internet Service Provider.
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is permitted
- Staff will be issued with a school phone where contact with pupils is required

How should personal data be protected?

The Data Protection legislation requires that data is**:**

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures

Please refer to the school's Data Protection (GDPR) policy for more information.

Online Safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn
- Our pupils' access to the Internet will be by adult demonstration with opportunities for the children to work directly on the Internet individually or with a partner. This will always be directly supervised by a teacher or adult
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form when their child begins school. This information is then uploaded to SIMs and logs kept of children that are not to have any online publications. This can be reviewed at any time by a parent. Any changes to this permission form will need to be signed and dated and returned to the school office to be updated on our system.

- All staff will be notified of pupils that are not allowed to have any form of online publication at the beginning of the academic year and throughout when changes may occur.
- Pupils will not be issued individual e-mail accounts, but will be authorised to use a group/class email address under supervision

How will risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly
- The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy is monitored

How will e-safety complaints be handled?

- 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
- Pupils and parents will be informed of the complaints procedure
- All communications will be logged on CPOMS and relevant staff informed.
- Parents and pupils will need to work in partnership with staff to resolve issues
- Discussions will be held with the Police liaison officer to establish procedures for handling potentially illegal issues
- The Safer Internet police agency will be informed of any potentially unsafe practice.
- CEOPs referral may be made if there is a possibility of exploitation e.g. grooming

How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice
- Regular e-Safety guidelines and media updates will be shared with parents online to ensure a strong communication link is maintained. The importance of discussions around online safety are encouraged on a regular basis.

How will the policy be introduced to pupils?

- Rules for safe Internet access will be posted in all areas of the school with access to the internet. These rules will be carefully written and illustrated to ensure all children understand their message. Children from the School Council will be involved to ensure these rules are approved by children, for children
- Pupils will be informed that Internet use will be monitored

- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use. Instruction in responsible and safe use should precede Internet access.

How will the policy be discussed with staff?

- All staff must accept the terms of the 'Acceptable Use Policy' statement before using any Internet resource in school
- All staff will be given the school e-Safety Policy and its importance explained to them. The whole staff will also be involved in the confirmation of the final draft of this policy before release to parents and children
- Staff will be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- The monitoring of Internet use is a sensitive matter. Members of staff that operate monitoring procedures should be supervised by senior management
- Staff development in safe and acceptable use of the Internet and on the school E-Safety Policy will be provided as required
- Staff are actively encouraged to maintain a high awareness of online safeguarding issues and asked to complete online training regularly.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school e-Safety Policy in initial letters and newsletters and from then onwards; the school website
- The use of TheSchoolApp and social media platforms will be used to communicate and identify current online risks
- Internet issues will be handled sensitively to inform parents without alarm
- A partnership approach with parents will be encouraged. This includes parent Internet safety information evenings which would include demonstrations, practical activities and suggestions for safe home Internet use

Pupils' e-Safety Agreement

For my own personal safety – everywhere!

- I will only use IT equipment when instructed to do so.
- I will ask permission from a member of staff before using the Internet at school.
- I am aware of "Stranger Danger" when on line and will not agree to meet online friends.
- I will tell an adult about anything online which makes me feel uncomfortable or unsure.
- I will not try to reach websites the school has blocked.
- I understand that the school may check my files and may monitor the web pages I visit.
- When in school I will only contact people with my teacher's permission.

- I will be very careful when sharing pictures or video of myself or my friends. If I am in school, I will always check with a teacher.
- I will not put any of my "Personal Information" online. (My full name, birthday, phone number, address, postcode, school etc.)

To keep the system safe

- I will only use my own login and password, which I will not let anyone else know.
- I will not access other people's files.
- I will not play games on a school device unless my teacher has given me permission.
- I will not install software on school device.
- I will not attach any equipment to the school devices, such as memory sticks.
- I will not use the system for gaming, gambling, shopping, or uploading videos or music.

Responsibility to others

- The messages I send will be polite and responsible.
- I will not upload images or video of other people without their permission.
- Where work is copyrighted (including music, videos and images,) I will not either download or share with others.
- I understand that the school may take action against me if I am involved in inappropriate behaviour on the internet and mobile devices.

Personal Devices

- The school cannot accept responsibility for loss or damage to personal devices.
- It is not permitted for pupils to use mobile phones during the school day. Mobile phones should not be brought into school unless there is a genuine reason for doing so and my parents have approved this.

- If I have to bring my mobile phone into school, I will hand it to the class teacher at registration and get it back at the end of the school day. This may be stored in the school office.
- Other devices (e.g. Games consoles, cameras) should not be brought into school, unless my teacher has given me permission.

Pupils' e-Safety Contract

Please complete, sign and return to the class teacher.

Pupil: _____Class: _____

Pupil's Agreement
I have read and I understand the pupils e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe.

Signed: _____ Date: _____

Parent's Consent
I have read and understood the e-safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school, advice for parents is available at www.saferinternet.org.uk or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I will ensure that any pictures taken during school events that include other children will not be shared using social media.

Signed: _____Date: _____

Please print name: _____