E-safety Policy

Ratified by trustees: December 2024

To Be Reviewed: December 2025

E-safety involves pupils, staff, trustees and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment at Westminster Primary School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

E-safety Policy

Our E-safety policy has been written by the school, following government guidance. It has been agreed by senior management and approved by trustees.

- The school's e-safety leader is Yogita Patel
- The e-safety trustee is Mr Nadeem Bhatti.
- The e-safety Policy and its implementation shall be reviewed annually.

Roles and Responsibilities

Headteacher and Senior Leaders:

- The headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-Safety will be delegated to the e-safety leader.
- The headteacher / e-safety leader will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The headteacher and senior leadership team (SLT) should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The e-Safety leader:

Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy / documents.

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

- Provides training and advice for staff
- Liaises with the school's ICT Operations Manager
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attends relevant meetings with the Safeguarding team and attend training sessions for recent updates.

Teaching and Learning

The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience:

- The school internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning, they will have been checked for appropriateness by the teacher setting the learning

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a diverse society.

Why is internet use important?

We use the internet for a number of reasons:

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The internet is a part of everyday life for education, business and social interaction.
- 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 need to learn how to evaluate internet information and to take care of their own personal safety and security whilst online.
- 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 functions.

Benefits of using the internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- 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 across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Local Authority and DFE

How can internet use enhance learning?

- The school's internet access will be designed to enhance and extend education.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

- The schools will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- 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 taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Authorised Internet Access

By explicitly authorising use of the school's internet access pupils, staff, trustees and parents are provided with information relating to e-safety and agree to its use:

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and internet access can be used within the school.

World Wide Web

The internet opens up opportunities and is becoming an essential part of the everyday world for children: learning, homework and sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the headteacher, by recording the incident in an e-safety log, which will be stored in the e-safety leader's office. The e-safety log will be reviewed termly by the e-safety leader.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Access in school to e-mail externally should be through the schools Office 365 email account.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social Networking

Social networking internet sites (such as Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered except for Twitter which can be used for school trips etc.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The trustees will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Home Learning

E-safety is maintained during home learning in the following ways:

- Lessons are recorded by teachers and quality assured by senior leaders before uploading.
- Lessons are uploaded only to our own website without any external links.
- Pupils and families provide feedback via a specific email address which is particular to a given year group.

Mobile Phones

Many mobile phones have access to the internet and picture and video messaging. They present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45am and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use a school phone to contact parents.
- Staff can use their phones for multi factor authentication (MFA) access.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers within the Foundation Stage place their phones in a locked cabinet in Nursery and Reception for the duration of hours worked by each member of staff. The remainder of staff ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom during the lunch period.
- Parents cannot use mobile phones on school trips to take pictures of the children.

Digital/Video Cameras

Pictures, videos and sound are not directly connected to the internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.
- The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Data protection

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

- The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- 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.
- This section is a reminder that all data from which people can be identified is protected.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

How will monitoring and filtering be managed?

The school will work with Exa, Entrust and Securus to ensure that systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Leader or a senior member of staff.
- The school's broadband access includes filtering appropriate to the age and maturity of pupils. The ICT/e-safety leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that staff believe is illegal must be reported to the headteacher/safeguarding lead who will inform the appropriate agencies.
- We keep up to date with new technologies, including those relating to mobile phones and handheld devices, to develop appropriate strategies.
- There are dangers for staff however if personal phones are used to contact pupils or families and therefore this will only be done when authorized by a senior member of staff.
- Abusive messages should be dealt with under the school's behaviour and anti-bullying policy.
- Emerging technologies will be examined for educational benefit and the headteacher in consultation with staff will give permission for appropriate use.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.

- Pupils are not allowed to bring mobile phones into school. If a child brings in a phone the teacher will remove the device from the pupil, the mobile phone will be kept in the school office. Parents/an adult will then have to come into school and collect it. The school will accept no liability for any lost/stolen phones.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos 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.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Parents may upload pictures of only their own child only onto social networking sites.
- The Trust Board may ban the use of photographic equipment by any parent who does not follow the school policy.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password needs to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

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 a school computer. The school does not accept liability for the 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.

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 shall be dealt with in accordance with school child protection procedures.

Communication of Policy

Pupils:

- Rules for Internet access will be communicated to pupils.
- Pupils will be informed that internet use will be monitored.
- Pupils will be informed when they are in KS2 of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during ICT lessons.

Staff:

- All staff will be made aware of the school e-safety policy.
- Staff should be aware that internet traffic can be monitored and traced to the individual user.
-

Parents:

- Parents' attention will be drawn to the school e-safety policy on the school website. They will also receive regular updates on e-safety.

Further Resources
We have found these web sites useful for e-safety advice and information.

www.thinkuknow.co.uk

www.childnet-int.org

www.kidsmart.org.uk

www.safesocialnetworking.com

Appendix 1:

Adult Internet and Acceptable Use policy Agreement

Whilst our school promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. **Using technology in school**

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other pupils, staff or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the GDPR.
- I will delete any chain letters, spam and other emails from unknown sources or speak to the ICT Operations Manager if unsure, without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.

- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the ICT Operations Manager or headteacher.
- The ICT Operations Manager will ensure any school-owned device is protected by anti-virus software and I will notify the ICT Operations Manager if there are any issues with anti-viral software on any school owned devices in my possession.
- I will only use recommended removable media and will keep this securely stored in line with the GDPR.
- I will only store data on removable media or other technological devices that has been encrypted of pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary, and which is encrypted.
- I will provide removable media to the ICT Operations Manager for safe disposal once I am finished with it.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes during contact time.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored in a safe place e.g. lockable storage.
- I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.

- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the headteacher or ICT Operations Manager.
- I will not use personal mobile devices to communicate with pupils or parents.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised and give permission for the ICT Operations Manager to erase and wipe data from my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites during contact time.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.

- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not give my personal details such as home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Working at home

- I will adhere to the principles of the GDPR when taking work home.
- I will ensure I obtain permission from the headteacher or the data protection officer (DPO) before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the ICT Operations Manager before it is used for lone-working.
- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
- I will act in accordance with the school's E-Security Policy when transporting school equipment and data.

5. Training

- I will ensure I participate in any e-safety or online training offered to me and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the ICT Operations Manager and SBM to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the E-Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the headteacher.
- I understand that the school will monitor my use of the ICT systems, email and other digital communications and recognise the consequences if I breach the terms of this agreement.
- I understand that the Trust may decide to take disciplinary action against me in accordance with the Staff Disciplinary Policy, if I breach this agreement.

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Signed: Date:

Print name:

DEVICE 1 Type of device: _____

Model Name: _____

Serial Number: _____

DEVICE 2 Type of device: _____

Model Name: _____

Serial Number: _____

DEVICE 3 Type of device: _____

Model Name: _____

Serial Number: _____