WILLIAM BARNES PRIMARY SCHOOL

E-Safety Policy

Reviewed by Curriculum Committee:	19.1.26
Approved by the Full Governing Body:	23.3.26
Next review due:	April 2027

Excellent teaching gives children the life chances they deserve; children learn better when they are engaged with their learning and we endeavour to achieve this through high-quality teaching. Education is for all, not the few as all children have the right to be the best they can be. At William Barnes, we aspire to foster a love of learning alongside the development of the well-rounded child.

Preparing Children for Life

We believe that we are preparing children for successful futures. We aim for them to be independent thinkers, confident, interested learners and global citizens, equipped to live, work in and contribute to society.

At William Barnes Primary School, we believe that children deserve:

- A strong sense of belonging fostered through positive relationships;
- High-quality feedback that moves their learning forward;
- Appropriate support to overcome specific barriers that they may face.
- Routines that provide consistency and stability throughout the school day.
- Children are able to be curious about different areas of learning.
- Children are given the opportunity to experience the widest variety of the written and spoken word possible with a vocabulary rich curriculum and school experience.
- Academic and pastoral experiences serve to enhance

Knowledge and Skills

As a school, we believe in the equal relationship between knowledge and skills in our curriculum. We believe that:

- Knowledge can be declarative (to know that) or procedural (to know how to).
- Both these forms are important and that declarative knowledge is turned into procedural knowledge through action and the act of practising and applying.
- Skills can be procedural knowledge as a result of the application of declarative knowledge.
- Skills can be linked to dispositions and behaviours.

In short, skills often procedural knowledge and are linked intrinsically to declarative knowledge.

We prefer to see the debate laid out as:

Knowledge → Comprehension → Application → Evaluation

Parents and carers

Evidence shows that *"Parental engagement has a positive impact on average of 4 months' additional progress."* (EEF) Parents and Carers are a vital part of the learning process at every step of a pupil's journey through our school therefore we work together with families to support their children's learning.

"For all children, the quality of the home learning environment is more important for intellectual and social development than parental occupation, education and income. What parents do is more important than who parents are." (EPPE)

This policy should be read in conjunction with other school Health and Safety policies, Safeguarding, Child Protection and Use of Mobile Phones in school Policies and the staff Code of Conduct and including Personal Safety and the Acceptable Use Policy.

Vision and Mission

1. At William Barnes Primary School, e-safety is integral to the school's overarching vision and mission. The school is committed to safeguarding all pupils, including in their use of digital technologies. This E-Safety Policy sets out the procedures and measures in place to ensure the safe, responsible, and secure use of the internet and information technology, including raising awareness of online risks such as misinformation and AI-generated content. Through this, the school seeks to protect children from potential harm and support them in developing the skills to critically evaluate digital information.

General

2. This policy applies to all members of William Barnes School community (including staff, governors, pupils, volunteers, parents, carers, visitors and community users).

3. The Education and Inspections Act 2006 empowers Head Teachers, to such an extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

4. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate behaviour that take place out of school.

Roles and Responsibilities

5. The Governing Body is responsible for the approval of the E-Safety Policy and for ensuring its ongoing effectiveness. A designated governor has specific responsibility for e-safety and will undertake regular monitoring and oversight. This includes attending relevant meetings, reviewing e-safety incident records and filtering logs, and reporting findings to the appropriate Governing Body committee to support effective governance and accountability.

6. The Head Teacher holds overall responsibility for the safety and wellbeing of all members of the school community, including in relation to e-safety, and will ensure that appropriate monitoring arrangements are in place. In their role as Designated Safeguarding Lead, the Head Teacher is suitably trained in e-safety and safeguarding matters, including through regular engagement with recognised training such as that provided by the Child Exploitation and Online Protection Centre (CEOP). The Head Teacher is aware of the potential for serious safeguarding concerns to arise from the use of ICT systems and the internet, including risks associated with misinformation and AI-generated content, and ensures that these risks are effectively managed. The Deputy Designated Safeguarding Lead is also appropriately trained to support this responsibility.

7. The Head Teacher and Senior Leaders will ensure that a planned programme of e-safety training is provided for all staff and that all members of the school community are made aware of the school's E-Safety Policy. They will monitor reports regularly and ensure that clear procedures are followed in the event of a serious e-safety allegation involving a member of staff. Senior Leaders will also ensure that e-safety newsletters are made available on the school website for parents to access. Training and guidance will include awareness of misinformation, including AI-generated content, to support staff and families in identifying and responding to inaccurate or misleading online information.

8. Teaching and Support Staff are responsible for maintaining an up-to-date awareness of e-safety matters, including current school policies and procedures. All staff must read and sign the Staff Acceptable Use Policy and must report any suspected misuse or concerns to the Head Teacher without delay. All digital communication with pupils and parents must remain professional in tone and must only take place through official school systems.

9. The ICT Technician will ensure that the school ICT infrastructure is secure, that the school meets the e-safety technical requirements, that users may only access the school's network through a properly enforced password protection policy and that the use of the RMUnify email is monitored.

10. Pupils will use the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they sign before being given access to the school systems, understand the importance of reporting abuse and how to do so, adopt good e-safety practice in and out of school.

11. Parents will make every effort to understand the issues and will be responsible for signing the Pupil Acceptable Use Policy. New parents to the school will be given an acceptable use policy as part of their entry pack. These will be stored in the Head Teacher's office in each child's personal file. Each member of staff, governors and volunteers will need to sign the acceptable use agreement and these will be stored centrally in the school office.

Policy Statements

12. A planned e-safety programme will be delivered through the Computing and PSHE (SCARF) curriculum areas and will address the safe use of information technology both in and out of school.

13. Key e-safety messages will be reinforced through a planned programme of assemblies and lessons, including twice-yearly E-Safety Weeks.

14. Pupils will be taught across the curriculum to develop critical awareness of the information they access online, including AI-generated misinformation, and will be supported to check the accuracy and reliability of sources.

15. The school will provide information and guidance for parents and carers through letters, the school website and parents' meetings. Parents will also be made aware of the SWGFL "Golden Rules" for parents, and the Head Teacher will share regular updates through weekly 'Wake Up Wednesday' communications.

16. Staff will act as positive role models in their use of ICT, the internet and mobile devices. Personal mobile devices should not be used in school in the presence of children, except in exceptional circumstances such as an emergency on a school trip when the school mobile phone is unavailable, in line with the school's Code of Conduct and Mobile Phones in School Policy.

Curriculum

17. E-safety should be embedded across the curriculum and reinforced by staff in all areas where digital technology is used. All staff should promote e-safety consistently through their teaching and modelling of safe, responsible ICT use.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, pupils should be made aware of the risks involved in publishing their own images online, including on social networking sites.

To safeguard the school community against misinformation, including AI-generated misinformation, pupils and staff should be taught to critically evaluate digital content and to recognise when information may have

been created or altered using artificial intelligence. The school will promote responsible research practices, encourage the verification of sources, and provide guidance on distinguishing reliable information from manipulated or false material. Staff will regularly review online safety education to ensure pupils develop the skills needed to question, report and avoid misinformation in digital environments.

SWGFL 360 E-safety Audit

18. The E-Safety Committee consists of the head teacher, the E-Safety Governor and the IT coordinator complete the SWGFL 360 E-safety audit at least annually and use this as a tool to guide the development of E-Safety. Following this year's audits a number of refinements to E-safety practice have been put in place

- A member of the school council has been elected as the E-Safety school councillor.
- An E-Safety school council meeting is planned, and the minutes will be discussed as an agenda item for the E-Safety Committee.
- Ensure all staff are using unique passwords that are private and not shared
- Staff use encrypted data sticks
- Staff are expected to use their staff e-mail address for all school related communications
- Initials should be used for all references to children in e-mail communications
- Staff to only use school approved encrypted data sticks
- With parental permission children may bring a Smart phone to school but this must be stored in the school office and collected at the end of the day

Internet Content Filtering and PREVENT

19. The school has adopted the SWGFL content filtering system as part of its Superfast Broadband package. Sites unsuitable for an educational setting are blocked automatically including sites which promote terrorism and extremism. Any sites which are not automatically filtered can be blocked by contacting SWFL administrators. Staff have undergone PREVENT training.

20. Staff can switch off the SWGFL filtering system to access web sites which are routinely blocked such as YouTube for educational purposes only. Staff bypass the filtering using a proxy server with a unique password and username for each member of staff. Staff must not leave a computer unattended and logged in. Use of the staff proxy is monitored to ensure inappropriate content is not accessed using school devices or using the school's internet connection.

Use of Digital Images

21. Digital images of children participating in events such as sports matches and fundraising events, are used from time to time on the school web site. Parents are given the opportunity to say that their children's image should not be used electronically on entry in reception and when joining the school at other times. Parents should not record digital images of children unless they are formally told that they can by a member of staff. At all public events parents are asked to refrain from uploading images unless they are of their own children exclusively.

E-Safety Week and Questionnaires

22. Annually during E-Safety week a questionnaire has been completed by children across the school allowing the monitoring of the use of IT out of school by children to help to ensure that children are not at

risk. During this week, an E-Safety assembly is held, parents are invited to an E-Safety meeting to discuss the latest developments from CEOP, and each class dedicates at least one lesson to E-Safety. During Staff meeting time in the run up to E-Safety week, staff are shown new resources and given updates on the latest trends in E-Safety.

Data Protection

23. Staff must ensure that they:

a. At all times take care to ensure the safe keeping of personal data, minimising the risk of loss or misuse.

b. Use personal data only on secure password protected computers and other devices, ensuring that they are properly logged off at the end of any session in which they are using personal data.

c. Transfer data using encryption and secure password protected devices.

d. Ensure that personal and confidential information is not stored on data sticks or other forms of portable storage unless they are password protected and encrypted.

Communications

24. Staff must use their school e-mail addresses for school related business.

25. Users need to be aware that email communications may be monitored.

26. Users must immediately report to the nominated person in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature, and must not respond to any such email.

27. Any digital communication between staff and pupils or parents/carers (e-mail, chat, VLE etc) must be professional in tone and content. These communications may only take place on official school systems.

28. Staff should not use social media websites such as Facebook in a way that may bring the school into disrepute or tarnish their reputations as professionals.

29. Staff should not use social media (such as Facebook messenger) to communicate electronically (chat) with children from the school.

30 All Social Media sites are blocked by the school's filtering service. Staff are allowed to access Social Media using their own devices on the school site but will only be able to do so using their Smart phone network.

See also:

Staff and Volunteers Acceptable Use Policy

Pupil Acceptable Use Policy

Privacy Notice

Useful Information and Resources

https://swgfl.org.uk/online-safety/

https://www.ceop.police.uk/Safety-Centre/

SSCT E-Safety Newsletters

Thinkuknow website at (https://www.ceopeducation.co.uk/)

https://saferinternet.org.uk/

https://saferinternet.org.uk/professionals-online-safety-helpline

www.internetmatters.org

https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes

https://www.ceopeducation.co.uk/professionals/guidance/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/

https://learning.nspcc.org.uk/online-safety/online-safety-for-schools

https://www.iwf.org.uk/

https://assets.publishing.service.gov.uk/media/633e965fe90e0709d835c519/UKCIS_Online_Safety_Audit_for_ECTs_and_ITTs_final_2022.pdf

https://nationalcollege.com/institutions/national-online-safety

William Barnes

Where every child counts