WILLIAM BARNES PRIMARY SCHOOL
Bridge Street
Sturminster Newton
Dorset DT10 1BZ

Tel/Fax: 01258 472257
E: office@williambarnes.dorset.sch.uk
W: www.williambarnes.dorset.sch.uk

Vision.

An inspirational, stimulating and well-resourced environment. *Preparing all children for life.*
A safe and secure school at the heart of the community. *A high quality professional team.*
Inquiry, independence and enthusiasm for learning. *High standards of behaviour.*
Taking pride in all our achievements.

E-SAFETY POLICY
FOR WILLIAM BARNES PRIMARY SCHOOL

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 the E-Safety policy operates within the wider context of the school vision and mission statement. The school's primary purpose is to keep the children safe and the E-safety Policy records the steps the school has put into place to ensure the safety of children on-line and when using IT.

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 headteachers, 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 Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor, and they will attend regular meetings, monitor e-safety incident logs and filtering logs and report back to the relevant Governing Body committee.
6. The Headteacher is responsible for the safety (including e-safety) of all the members of the school community and will carry out the e-safety monitoring role. As Designated Safeguarding Lead she is trained in e-safety issues following regular attendance at Child Exploitation and Online Protection Centre training (CEOP) and is aware of the potential for serious child protection issues to arise from the use of ICT systems and the internet. The Deputy Designated Safeguarding Lead is also suitably trained.
7. The Headteacher and Senior Leaders will ensure there is a planned programme of e-safety training for all staff, and ensure all members of the school community are aware of the school's e-safety policy. They will regularly monitor reports and know the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. Senior staff will also ensure the Safe Schools Community Team E-Safety newsletters are uploaded to the school web site for parents to download.
8. Teaching and Support Staff are responsible for ensuring that they have an up-to-date awareness of e-safety matters and of the current school e-safety policies and practices. All staff members will read and sign the Acceptable Use Policy for staff and will report any suspected misuse or problem to the Headteacher. Digital communications with pupils and parents (e-mail, VLE or voice) must be on a professional level and only carried out using 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 Headteacher'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 is provided as part of the Computing and PHSE (Jigsaw) curriculum areas– this will cover both the use of Information Technology in and out of school.
13. Key e-safety messages should be reinforced as part of a planned programme of assemblies and lessons including twice yearly E-Safety weeks.
14. Pupils should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of the information.

15. The school will provide information and awareness to parents and carers through letters, Barnestorm (school magazine), website and parents'meetings. Parents should be made aware of the SWGFL "Golden Rules" for parents.
16. Staff should act as good 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 (See code of conduct and mobile phones in school policy) except under special circumstances such as an emergency on a school trip when the school mobile phone is not available.

Curriculum

17. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum. 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, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

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.

Appendices

Staff and Volunteers Acceptable Use Policy
Children's acceptable Use Policy
Pupil Acceptable Use Policy
Privacy Notice

Useful Information and Resources

SWGFL E-safety policy guidelines.
SWGFL Security Policy and Acceptable Usage Policy.
SWGFL Staying Safe
SWGFL 360 Safe online E-Safety review tool
CEOP web site
SSCT E-Safety Newsletters
Thinkuknow web site
UK Safer Internet Centre
Professionals Online Safety Helpline

Adopted date:	20th November 2023
Signature of Headteacher:	Karen Wrixon
Signature of Governing body:	Chris Jones
Next review date	Autumn 2024