Stebbing Primary School
E-Safety Policy

Created/updated: June 2024
Ratified By School Governing Body: June 2024
Due for Review: June 2027

This policy is aimed at children using computers within school. In the event of unplanned school closure and where online learning is required please see the Unplanned school closure section on page 5 and refer to our Child Protection Policy located on our school website
www.stebbingprimary.co.uk/policies

Introductory Statement

Our e-Safety Policy has been written to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The internet is considered an essential part of modern life. In addition, the school has a duty to provide pupils with quality internet access as part of their learning. This e-safety policy considers the use of both the fixed and mobile internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, and portable media players. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and risks will be assessed and managed accordingly.

Aims

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 systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use.

The school will ensure that all members of the school community are aware of the e-safety policy and the implications for the individual. E-safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of the internet and other communication technologies.

TEACHING AND LEARNING

How we manage the risks:

a) The school internet access is through the secure, filtered broadband from the Essex Grid for Learning (e-gfl).
b) A Virus protection system is installed on all computers in school and the school checks that this protection is updating regularly and informs the LA of any issues. Any portable media brought into the school must have permission from the Computing Subject Leader and will be subject to a virus check.
c) The school will work with the LA to ensure systems to protect pupils are reviewed and improved.
d) The Headteacher and subject leader ensures that the e-safety policy is implemented and compliance with the policy monitored. Some material available on the internet is unsuitable for pupils. Methods to identify, assess and minimise risks will be reviewed regularly. The school will take all reasonable precautions to ensure that pupils access only appropriate material. However, due to the nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
e) Where unsuitable content is encountered staff and pupils should follow the school procedures for such events. Report any instance of inappropriate sites that come through the filter system to the Computing Subject Leader, who will inform the Headteacher and the IT Consultant, so that they can be blocked. The IT Consultant will help the school to ensure the correct procedure and action is taken as required.
f) Emerging technologies will be examined for educational benefit and any risk considered before use in school is allowed.

h) The school systems use Google Education to store all cloud-based files, our school calendar and email accounts.

Internet use to enhance learning

1. Pupil access to the internet will be by adult demonstration or directly supervised access to specific, approved on-line materials. Instruction in responsible and safe use by pupils will precede internet access.

2. As part of the curriculum, pupils will be made aware of the guidelines for the acceptable use of the internet and what is not acceptable. These guidelines for acceptable use will be clearly on display in all areas of the school where internet access is available.

3. All pupils will be given clear objectives when using the internet. Where internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils.

4. All websites used for specific activities will have been approved by the class teacher and where necessary, the Headteacher.

5. Curriculum activities that involve the use of the internet for gathering information and resources will develop pupil skills in locating and evaluating materials. Pupils will be taught how to validate materials they read before accepting their accuracy.. Where materials gathered from the internet are used by pupils in their own work, they will be taught to acknowledge the source of information used. The school will ensure that the use of internet materials by staff and pupils complies with copyright law.

   6. During computing lessons, older children will be supported in creating Scratch accounts. This process will be preceded by instruction about how to create and use accounts safely and a teacher's email address will be associated with the account.

Email

1. Curriculum activities that involve the use of email will be through the use of class or group accounts that are controlled by the school.

2. The use of individual pupil personal accounts will not be permitted through the school system. Pupils will have their own Google accounts. They can only email people within our school community as part of curriculum lessons. Ability to e-mail other schools outside the county must be approved by a member of staff. As the children get older they may begin to use their email account out of school as a form of communication. However, children can only email to other members of the school with an @stebbingprimary account.

3. Pupils must immediately report to an appropriate member of staff if they receive any offensive email.

4. In email communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

PUBLISHED CONTENT

1. Parents/ guardians will be asked at the beginning of their child's time with us to give their permission for photographs taken in school to be used in the press or on the school website/twitter account.

2. Staff or pupil personal contact information is not published. The contact details for the school on our website is the main school office.

3. The school website is maintained and kept up to date. The Headteacher and Administration Assistants ensure that the content is accurate and appropriate to the needs of the school community.

SOCIAL NETWORKING AND PERSONAL PUBLISHING

1. The use of online chat rooms, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the pupils.

2. Pupils will always be advised never to give out personal details of any kind which may identify them, their friends or their location.

3. If Social networking sites such as Facebook, Twitter and Instagram are used outside of school, staff should not have any present pupils as their friends on such sites.

4. Children have the use of Class Dojo to showcase work. This is not for communication purposes.

OTHER TECHNOLOGIES

1. Pupils are not allowed to bring mobile phones into school. In the event of this happening these are kept in the school office until the end of the day. For older pupils who come to school by themselves parents can request that they bring their phone into school but with the understanding that it will be kept in the school office until the end of the day. This is to avoid the possibility of the sending of abusive or inappropriate text messages or accessing the internet not through a filtered system.

2. The school may use video/audio communication technologies to communicate with families.

https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

AUTHORISING internet ACCESS

1. All staff will need to agree to our e-safety policy before using any internet resource in school. Staff will be made aware that internet traffic can be monitored and traced to the individual user and professional conduct is essential.

2. Pupil access may be withdrawn if the acceptable use guidelines are not adhered to.

3. The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

COMMUNICATION OF OUR E-SAFETY POLICY

Introducing E-Safety to Pupils.

1. E-Safety rules will be discussed with the children at all appropriate ages.

2. Every time pupils use individual logins they will have to agree to our E-Safety Rules.

3. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

4. E-safety is covered at an appropriate age level at the beginning of each year.

5. As part of the school curriculum the pupils will participate in an internet proficiency training programme on a yearly basis with the 2 Johns.

Anti-Bullying Alliance
A place to help you boss your life online - Own It - BBC
UK Council for Internet Safety - GOV.UK
Online Safety Resources for Teachers - Be Internet Legends

STAFF and the E-safety policy

1. All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school e-safety policy.

2. All staff will be required to agree to our e-Safety policy.

3. Staff development in safe and responsible internet use will be provided as part of the continuing professional development programme and attend a workshop with the 2 Johns on an annual basis

4. All staff can have approved internet access.

5. Staff will always use a child friendly safe search engine when accessing the web with pupils.

6. In order to enable safe practice, staff should ensure their settings on social media sites are secure.

8. Staff should not access the internet for personal use during class based time at school.

9. Staff should not be using mobile phones for personal use during class based time.

E-safety complaints

Where incidents occur due to non-compliance with the school e-safety policy these will be reported to a delegated senior member of staff. Any issues relating to staff misuse must be referred to the Headteacher. Should it become necessary to prohibit the use of internet resources for a pupil then parents or carers will be involved so that a partnership approach can be used to resolve any issues. This could include practical sessions and suggestions for safe internet use at home.

E-safety for parents

1. This policy is on the schools website for parents to access.

2. Annually the school will send out relevant e-Safety information to parents including offering the opportunity to attend a workshop run by the 2 Johns.
3. Regular updates to be posted on Class dojo relating to apps, games and websites that children may have access to at home.

4. Staff need to be aware that situations could arise when communicating or becoming friends with parents on social media sites. Therefore this needs to be carefully considered before doing so.

Report to CEOP
The use of social media for online radicalisation - GOV.UK
Parent Zone