East Sheen Primary School

Online Safety Policy

1. Introduction

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to online safety. The policy relates to other policies, such as: Teaching and Learning, Anti- Bullying, Safeguarding & Child Protection, Home Learning and Health & Safety.

The Computing Leader is the designated Online Safety Coordinator. The online safety policy has been approved by the governors. It will be reviewed on an annual basis.

2. Teaching and Learning

The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the internet is a necessary tool for staff and students. It helps to prepare students for their on-going career and personal development needs. It is a requirement of the National Curriculum (NC) for Computing and is implied in other subjects.

Internet use enhances learning. Internet access is provided by the Local Authority (LA) and is designed for pupils. This includes filtering appropriate to the content and age of pupils. Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirement. Pupils are given clear objectives for internet use and sign an Acceptable Use Agreement in class. This is reviewed with the children during a computing lesson and the wording is shared with parents/carers. Staff select sites which support the learning outcomes planned for pupils' age and maturity.

Pupils throughout the school, from Reception to Year 6 are taught about the importance of internet safety through a number of means: within the PSHE curriculum, including relationships education; during Computing lessons; in school assemblies; and through identified awareness days, such as Internet Safety Day.. Pupils are taught how to take responsibility for their own internet access and how to evaluate internet content. They are taught ways to validate information before accepting that it is necessarily accurate and to acknowledge the source of information, when using internet material for their own use.

Pupils are made aware that the writer of an e-mail or the author of a web page might not be the person claimed. Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

3. Managing Internet Access

The school ICT system security is reviewed regularly. Virus protection is updated regularly. Security strategies are discussed with the Local Authority and our IT services provider.

Pupils are allowed to use school email accounts only. Pupils must tell a teacher immediately if they receive offensive email. In emails pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission. Pupils are taught not to open suspicious incoming email or attachments. The forwarding of chain letters is not permitted.

Governors review with school leaders the effectiveness of online filtering and the headteacher will report on any updates, in line with guidance from 'Keeping Children Safe in Education 2025'.

4. Password Policy

Staff and pupils should always keep their passwords private, must not share with others and if a password is compromised, the school should be notified immediately. All staff have their own unique username and private passwords to access school systems. We require staff to use STRONG passwords and to change their passwords regularly - for the school network every 6 weeks and the MIS (Arbor) every 90 days.

School laptops that leave the school premises are encrypted to provide additional protection if the computer is lost or stolen.

We require staff using critical systems to use two factor authentication. (e.g. LGFL Support Site) and do the same for sensitive safeguarding information (e.g. CPOMs).

5. E-mail

Staff are provided with an email account for their professional use - a Microsoft Office 365 account. We use anonymous or group email addresses, for example info@eastsheen.richmond.sch.uk as the main public point of contact for the school.

The school will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

We ensure that email accounts are maintained and up to date. We use a number of LGfL-provided technologies to help protect users and systems in the school, including LGfL's web content filtering product.

Staff will use Office 365 email systems for professional purposes. Access in school to external personal email accounts may be blocked.

Email is not used to transfer staff or pupil personal data outside of the school secure network unless anonymised. 'Protect-level' data should not be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

The Office 365 email system is also used by pupils, this includes Microsoft Teams. Throughout our computing curriculum, children are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

6. Published content and the school website

The headteacher, supported by the governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

The school website complies with statutory DFE requirements.

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

Photographs published on the web do not have full names attached and must not identify individual pupils. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website. Group shots are used in preference to individual "passport" style images. Children's photographs are only allowed to go on the website if permission is held from the child's parents/carers.

The contact details on the website are for school admin only.

7. Social networking and personal publishing

Reference should not be made in social media to pupils, parents/carers or school staff. School staff should not be online friends with any pupil nor should they engage in online discussion on personal matters relating to members of the school community. Any exceptions must be approved by the headteacher.

Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

The school works in partnership with parents, the LA and our Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Pupils will not be allowed to access public chat rooms. New applications are thoroughly tested before pupils are given access. Pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work. Pupils are required to follow our [age appropriate] KS1/KS2 Acceptable Use Agreement. The agreements are signed in class and appear as a reminder (pupils are prompted to accept) when logging onto the school system.

Senior staff ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the computing lead.

Parents/carers are asked to acknowledge their responsibility for setting standards with their child around internet use in our registration document and through additional communication materials as required. Whilst the school strives to educate our pupils about appropriate online behaviour, parents/carers are responsible for their online use outside of school. The school website has online safety resources to support parents and children on the website at the link. This includes materials from the parent meeting hosted by the school with a specialist advisor.

8. Sharing nudes or semi-nudes or 'Youth Produced Sexual Imagery'

If an incident of sharing nudes or semi-nudes (sometimes known as 'sexting') or 'youth produced sexual imagery' is discovered or reported within school, then the school will respond in line with its Child Protection and Safeguarding Policy, following also the recommendations of UKCCIS (UK Council for child Internet Safety) in 'Sexting in Schools and Colleges', see link.

9. Online bullying

9.1 Definition

Online bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. See also the school behaviour policy and anti-bullying policy.

9.2 Preventing and addressing online bullying

To help prevent online bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss online bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online bullying, as well as other aspects of online safety. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on online bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on online bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected. This is included by linking the newsletter to parent/carer resources from the National College's 'National Online Safety' bank.

In relation to a specific incident of online bullying, the school will follow the processes set out in the school behaviour policy and anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will follow the processes set out in the 'Child Protection and Safeguarding' policy.

9.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the school's behaviour policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL.

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the headteacher / DSL / other member of the senior leadership team, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour and child protection and safeguarding policies

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

East Sheen Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

East Sheen Primary School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, which must be agreed by the Headship Team.

10. Mobile phones and cameras

Mobile phones must not be used by pupils during the school day and they are required to hand their phones to their class teachers during the day for safe keeping. Staff will use mobile phones in line with staff Code of Conduct. Students are not permitted to bring smartphones to school and parents/carers will need to provide a non-smart or 'brick-style' phone instead.

The sending of abusive or inappropriate text messages is forbidden. Cameras in mobile phones are not used by staff or pupils. Only school cameras are used by both staff and children for educational purposes. (Please refer to the Parent Helper guidelines for guidance on the use of cameras and mobile phones by parents and carers in school).

11. Data Security

The headteacher is the Senior Information Risk Owner (SIRO).

Judicium Education is the Data Protection Officer

The key contact(s) for key school information (the Information Asset Owners) are the School Business Manager and the Computing Leader.

Staff must report any incidents where data protection may have been compromised to the Headship Team.

Staff have secure area(s) on the network to store sensitive files.

We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.

Office 365 email accounts are automatically created for staff and pupils on their entry to the school (when desktop/laptop login accounts are created on the internal school system) and will be deleted when they leave the school.

We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.

All servers are in lockable locations and managed by DBS-checked staff.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2013.

https://www.legislation.gov.uk/uksi/2013/3113/contents

Where any protected or restricted data has been held on a server a certificate of secure deletion will be obtained. Secure file deletion software is used.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

12. Policy Decisions

All staff must read and sign the "Acceptable use Policy" before using any school ICT source, and are reminded when logging onto school devices by the device. The school maintains a record of all staff and children who have access to the school's ICT systems. Any person not directly employed by the school will be asked to read and sign the "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

The school takes all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access. The school's Online Safety Policy and its implementation will be monitored and reviewed on a regular basis.

Complaints of internet misuse must be referred to the headteacher. Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with the school's Child Protection and Safeguarding Policy. Pupils and parents are informed of the complaints procedure.

13. Communications Policy

Online safety reminders appear on screen as children log into computers. Pupils are informed that network and internet use is monitored and appropriately followed up.

All staff are trained regularly and receive a copy of the Online Safety Policy. Staff are informed that network and internet traffic can be traced to an individual user. Staff will use an age appropriate search engine when accessing the web with pupils.

Parents' and carers' attention is drawn to the school's Online Safety Policy and Acceptable Use Policy. The school has links on its website to online safety resources. The school seeks to engage with parents and carers on the issue of online safety and information evenings are offered by school on a regular basis.

14. CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission. See 'CCTV Policy'.

We use lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

The following government guidance is to be considered in conjunction with the above-written policy:

- Teaching online safety in schools
- Preventing and tackling bullying
- Relationships and sex education
- Searching, screening and confiscation
- Protecting children from radicalisation
- Online Safety Act 2023

Approved by governors: Spring 2026
Review date: Spring 2027