Goldsworth Primary School

Online Safety Policy

Writing and reviewing the Online Safety Policy

The Online Safety Policy is part of the Trust and School Development Plans and relates to other policies including those for Computing, Anti-bullying and for Child Protection.

- The Designated Safeguarding Leaders and Computing Leader are responsible for this policy.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management.
- The Online Safety Policy and its implementation will be reviewed every 3 years or earlier if changes are needed
- The Online Safety Policy covers the use of all technology that can access the school network or the Internet, or which facilitates electronic communication from school beyond the bounds of the school site.

Managing Internet Access

The school will provide managed Internet access to its staff, children and visitors in order to provide a secured and protected Internet experience whilst allowing children to learn how to assess and manage internet risk; to gain the knowledge and understanding to keep themselves safe when using the Internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will ensure that all Internet access has age appropriate filtering provided by a recognised filtering system, which is regularly checked to ensure that it is working, effective and reasonable.
- The filtering systems currently in use are Smoothwall and Senso.
- All internet activity, regardless of the user or device, is recorded and retained, and reports of this activity can be viewed and monitored by staff in the appropriate roles. The school DSL(s) review these reports daily.
- For serious activity breaches, instant reporting is enabled to alert the school DSL(s) immediately without waiting on a daily report check.
- School ICT systems security will be reviewed regularly.
- The school will ensure that its networks have virus, malware and ransomware protection and will ensure that this is updated regularly.

Authorising Internet access

- All staff (any approved person who is working or volunteering for the school or the trust) must read and sign the staff 'Acceptable Use Policy'.
- The school will maintain a current record of all staff and children who are granted access to school computing systems.
- If a professional visitor requires internet access, they are given access to a separate monitored Guest/BYOD wifi network.

- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.

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 device. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- Our school will monitor computing use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

Handling Online Safety complaints and Online Safety risks

- Complaints of Internet misuse will be dealt with by an appropriate member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with the child protection and safeguarding procedures as outlined in the Safeguarding policy.
- Children, parents and carers will be informed of the complaints procedure.
- Children, parents and carers will be informed of consequences and sanctions for children misusing the Internet and this will be in line with the school's behaviour policy.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety policy.

Communication of the Policy

Introducing the Online Safety Policy to Children

- Appropriate elements of the Online Safety policy will be shared with children.
- Online safety rules will be posted in all networked rooms.
- Children will be taught about online safety regularly throughout the year.
- Children will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for children. This should be addressed each year as children become more mature and the nature of newer risks can be identified.

Staff and the Online Safety policy

- All staff will read the school's Online Safety Policy and its importance explained.
- All staff must sign and agree to comply with the Acceptable Use Policy in order to gain access to the school computing systems and to the Internet.

- Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff are responsible for the appropriate usage of their computer and school devices- for protecting passwords and managing personal information in line with GDPR.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters and on the school website.
- Parents and carers will be provided with additional information on Online Safety at various times throughout the year.
- Parents and carers will have the opportunity to attend an Online Safety information session once a year.
- Parents and carers will be asked to sign an 'ICT Usage Policy and Agreement' when children begin school, which outlines the use of the internet in school and at home.

Teaching and learning

Internet Use

Our school will provide an age-appropriate online safety curriculum that teaches children how to stay safe; how to protect themselves from harm and how to take responsibility for their own and others' safety. This will be taught across all year groups. All communication between staff and children, or families will take place using school equipment and/or school accounts. Children will be advised not to give out personal details or information that may identify them or their location.

Internet and Digital Communications

- The Internet is an essential element in 21st century 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
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Parents and carers will be asked to sign an 'ICT Usage Policy and Agreement' when children begin school, which outlines the use of the Internet in school and at home.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children will be shown how to publish and present information appropriately to a wider audience.
- Children are educated on how to stay safe online outside of school through our online safety lessons. These include how to stay safe on social media.
- Parents and carers are educated on how to keep their children safe online through external visitors and regular updates are sent home.

Children will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by children complies with copyright law
- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children will be taught how to report Internet content that makes them feel uncomfortable to a responsible adult.
- Children will be aware of the risks and benefits of Artificial Intelligence.

E-mail

- Children and staff may only use approved e-mail accounts on the school system.
- Staff will only use their work email to send and receive school related emails, email external agencies and parents.
- Staff to pupil email communication must only take place via a school email address and will be monitored.
- Incoming email should be treated as suspicious and attachments not opened and links not clicked unless the author is known and an assessment of the legitimacy of the content is made.
- Children will be encouraged to tell a teacher if they receive an email that makes them feel uncomfortable.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Children can only send email to other staff and children within their school or federation.
- Children can receive email from staff or children within their school or federation.
- All email sent to and received from a child's accounts is stored and retained until the email account is deleted e.g. when the child is taken off roll.

Published content

- The contact details on website(s) should be the school or trust address, generic email and telephone number. Staff or children' personal information or name specific email addresses will not be published.
- The nominated staff will take overall editorial responsibility and ensure that content is accurate and appropriate regardless of the content platform

Publishing children' images and work

- Parents and carers will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- Written permission will be obtained from parents or carers during the admissions process before photographs of children are published on the school website or other platforms.

- Publishing children' full names will be avoided, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Parents and carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking

- The school will educate children in their safe use of the Internet and Social Media.
- Children will not be able to access social networking sites whilst at school, however, the school will consider how to educate children in their safe use e.g. use of passwords and not sharing any personal information.
- Children will be advised never to give out personal details of any kind which may identify them or their location.
- Children and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged children.
- Children will be advised to use nicknames and avatars when using social networking sites
- Children will be encouraged to tell a parent or carer if they receive any form of communication via Social Media outside of school that makes them feel uncomfortable. Children will also be supported at school as appropriate.

Managing filtering

- If staff or children come across unsuitable online materials, the site must be reported to a member of the safeguarding team. If a pupil reports an issue to their teacher, this then must be followed up by reporting to a member of the safeguarding team.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Smoothwall and Senso monitoring software will monitor and record any inappropriate material that is accessed by staff, children or visitors. It will store all internet activity for a period of 3 months and alerts the members of the safeguarding team immediately, on a daily basis, via email. Individual system users are able to be monitored and investigated as needed through producing a report of their internet activity and online searches. Daily flagged items are investigated and recorded on CPOMS if further action is required. If further action is required then the DSL will be informed and safeguarding procedures will be followed (see Safeguarding policy).

Managing video conferencing

- Children should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the children's age.
- Schools will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Additional statements

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff must use a school phone where contact with parents, children and other school related matters is required.
- The use of tablets and Google Chromebooks is monitored as part of our Acceptable Usage Policy.
- Staff are not to use personal and\or non-school owned\controlled devices to take or store images of children, or pupil personal data.

Protecting personal data

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

School's Procedures in relation to mobile phones

- Children should only need to have mobile phones to contact parents as they walk home to/from school by themselves.
- If children bring mobile phones to school, they must be given to the class teacher for safekeeping until the end of the day.
- Mobile phones must only be used by children for appropriate purposes.
- Staff and visitors are not to use their personal mobile devices whilst around the children, except where such use is for a required school function e.g. multi-factor authentication or in an emergency when on an off-site school trip.

Sharing Nudes and Semi Nudes (formally Youth Produced Sexual Images)

The practice of children sharing images and videos via text message, email, social media or mobile messaging apps has become commonplace. However, this online technology has also given children the opportunity to produce and distribute sexual imagery in the form of photos and videos. Such imagery involving anyone under the age of 18 is unlawful.

If inappropriate messages or images are found (or staff are told about them) the following action will be taken:

1. The device will be confiscated by staff and taken to a Designated Safeguarding Lead (DSL).
2. The image will not be viewed by staff unless necessary; in which case this will be viewed by the DSL and another member of the Senior Leadership Team only.
3. The DSL will investigate the situation by discussing with the relevant members of staff.
4. The DSL will interview the children involved.
5. The DSL will meet with the parents of the children involved (unless this puts the pupil at greater risk).
6. A referral may be made to CSPA (Children's Single Point of Access) or the Police.

7. If no referral is required, the image will be deleted from the device and returned to the pupil.
8. The DSL will arrange necessary support for the pupil.

Policy Decisions

Date written: September 2021

Prepared by: Elise Baird & Emma Knight

Reviewed: Jan 2026

Next review (3 Years): Jan 2029