Onslow Infant School

Online Safety Policy

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

Governors' Committee Responsible:	Full Governing Board
Nominated Lead Member of Staff:	Katherine Donlon
Status & Review Cycle:	Statutory (Annual)
Next Review Date:	September 2025

Policy Review

This Policy was adopted Autumn 2024
The Policy will be reviewed in Autumn 2025

Learning and teaching

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- As an essential element for education, business and social interaction, the school has a duty to provide students with quality internet access as part of their learning experience.
- Children will be taught that the internet and digital technology has huge educational and social benefits when used safely.
- Through the computing and RSE curriculums, pupils will be taught about the potential dangers of internet use, including how to report unpleasant content.
- Pupils of all ages will be educated in the safe, effective use of the internet to support their learning and mental health.
- Pupils will be taught how to publish work to a wider audience on secure educational platforms including Purple Mash and Tapestry. Both platforms are password protected.
- For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience, acknowledging the lack of experience and internet at home.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.
- The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing internet Access

- The school internet is provided on a broadband contract.
- The school ensures that children remain as safe as possible by filtering or blocking access to sites which are inappropriate to the age of pupils.
- Filtering and blocking notifications are analysed and safer practice is reviewed as a result.
- School IT systems security will be reviewed regularly, with technical support and expertise.
- Virus protection will be updated regularly.
- The school will work in partnership with Surrey County Council to ensure that security systems to protect pupils are reviewed and improved.
- If the staff come across unsuitable materials the site must be reported to the Head Teacher and Computing Subject Leader.
- School Leaders will ensure that regular checks are made to ensure the selected filtering methods are appropriate, effective and reasonable.

Managing personal information online

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR Regulations (2018)

Email

- Governors may only use approved e-mail accounts on the school system for matters related to school. They may however receive notifications from the GVO platform and National College via their personal email.

- Staff may only use approved e-mail accounts on the school system for matters related to school.
- Pupils/parents/carers must immediately tell a teacher if they receive offensive e-mails linked to school.
- Staff to pupil/parent/carer email communication must only take place via a school email address or via 2Email on Purple Mash. Emails will be monitored except when the pupil is known to the member of staff in a capacity other than through school e.g. if a member of staff has a child at the school they may have other parents' details in order to arrange play dates.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Cc/Bc or inform Head Teacher of any e-mail deemed sensitive.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher, Leadership Team, School Business Manager and Admin Staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used on the website particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platforms

- The school will educate pupils in the safe use of social networking sites through the use of the Purple Mash and Tapestry e.g. use of emails/messages, usernames, passwords etc.,
- Pupils will be taught never to give out personal details of any kind which may identify them or their location.
- Pupils/parents/carers will be advised that the use of social network spaces outside school brings a range of opportunities; however it does present dangers for pupils.
- Facebook, Twitter, Instagram or other social networking sites, must not be used to share anything which may bring the school into disrepute. Staff must ensure that their personal privacy settings are locked down and remember that these settings need to be checked every time the site owners update the site.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Handheld devices such as ipads, will be connected to the school internet and any associated filtering.

- Apps downloaded from the Apple/Play store or similar will be checked for appropriateness and the learning they provide for the age groups and children that will be using them.

Mobile Device guidance

Onslow Infant School has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is securely held and complies with the requirements of the Data Protection Act 2018. The use of portable computer devices, including mobile phones, increases the risks associated with the secure storage of data.

General use of mobile phones

- Mobile phones and personally-owned devices will not be used in any way during lessons. They should be switched off or silent at all times. Unless as part of an approved and directed curriculum-based activity consent has been given by the Head Teacher.
- Use of mobile phones may be granted where there is a specific medical need and this is monitored by the device. However, the camera lens' will be covered.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- No images or videos should be taken on mobile phones or personally-owned mobile devices in school.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families in a professional capacity within or outside of the setting unless there are exceptional circumstances in doing so and permission has been granted by the Head Teacher.
- In exceptional circumstances such as school closure, the Head Teacher may give permission to staff to call parents and carers from their own phones. In this instance, the caller ID must be blocked. This can be done by keying in*67 before the telephone number.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode and kept out of sight of children. Mobile phones or devices will not be used during teaching periods unless permission has been granted by the Head Teacher in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the Head Teacher and under close supervision of an adult.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action will be taken as appropriate.
- Staff should ensure that their phones are password protected by a PIN, facial recognition, fingerprint or similar, in case of loss or theft.
- Staff should never give their mobile phone number to students/parents/carers – except when the parent /carer is a personal friend or a family member or is known to them in a capacity other than that through school. If a member of staff needs to make telephone contact with a parent/carer, a school telephone should be used unless express permission has been given by the Head Teacher in exceptional circumstances.

- Staff should never save parents/pupils/carers telephone numbers/email addresses on their mobile phone, as this allows the possibility of inappropriate contact unless this has been authorised by the Head Teacher.
- Staff should never send to, or accept from anyone, texts or images that could be viewed as inappropriate.

Policy Decisions

Authorising internet access

- All staff must read and sign the Staff Acceptable Use Agreement before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Access to the internet within school, will follow adult demonstration with access to specific, approved on-line materials via a class computer, ipad or other approved technologies.

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 computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.
- The school will monitor ICT 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

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher (or Chair of Governors if it relates to Head Teacher).
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure via the school website.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with this Online Safety Policy and Acceptable Use Agreement.

Communications Policy

Introducing the Online Safety Policy to pupils

- Appropriate elements of the Online Safety Policy will be shared with pupils
- Online safety rules will be posted in all networked classrooms.
- Pupils will be informed that 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 pupils.
- Online safety rules will be revisited each term as students become more mature and the nature of newer risks can be identified. Students will be reminded of the safety rules in each computing lesson if they will be accessing the internet.

Staff and the Online Safety Policy

- All staff will be given access to the Online Safety Policy and its importance explained.