Oatlands School

Online Safety Policy

Date of last review: Summer 2023
Date of next review: Summer 2025

Subject Leader at last review: Katy Wood

Policy Development

This Policy has been written by the Online Safety Leader. It follows the Surrey Model Online Safety Policy and CEOP guidelines. This document is a statement of the principles, aims and strategies for Online Safety at Oatlands school.

This policy applies to any person in school (e.g. Staff, Pupils, PTA members, parent helpers, volunteers, students)

This policy provides the guidance for the use of all electronic communication within the school including staff-staff, staff-pupil, staff-parent and parent-parent.

The Online Safety Leader will receive training to remain abreast of changes and new technology.

It was presented to the Governors in July 2015 and will be reviewed and updated annually.

This policy was updated May 2017.

This Policy was updated in November 2019.

This policy was updated in July 2021.

This policy was updated in May 2023.

The Online Safety Policy is part of the schedule of annual publications and reviews.

Links with other policies

- Computing Policy
- The Safeguarding Policy
- Pastoral Policy
- Staff Handbook
- Code of conduct
- PTA Reps letter
- Laptop agreement for staff
- Teacher's contracts
- Whistle Blowing Policy
- Handbook for Volunteers

Contents Page

Section 1: Introduction

Section 2: Roles and Responsibilities

Section 3: Teaching and Learning

Section 4: Managing Internet Access

Section 5: Communications

Living our Values, Learning for Life

1.1: Policy Statement

The internet is an essential element in 21st century life for education, business and social interaction. At Oatlands we have a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the integral curriculum and a necessary tool for staff and pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use as set out in the schemes of work. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to present information appropriately. Our Values based education allows our children to feel safe and secure when exploring technology and know and understand who they can talk to if needed.

1.2: Aims

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- To deliver an effective approach to online safety which empowers us to protect and educate the whole school community and its use of technology, including mobile and smart technology.
- To have clear mechanisms to identify, intervene and escalate an incident where appropriate.

To enable children to:

- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Ask for help if they are unsure or worried about something they see on the computer.
- Understand the importance of logging on and not sharing passwords or personal information.
- Treat people online as you would treat them in real life.
- Understand that the internet is not always safe so follow adult instructions when using the internet.

To ensure adults:

- Teach the children the safety rules on how to be safe when online
- Check videos/adverts before sharing to the class.
- Give clear instructions on using the internet.

Roles and Responsibilities

2.1: The governing body will:

- Work with the head teacher to ensure that realistic funds are made available to implement this policy.
- Identify one Governor as the designated Online Safety governor who will attend any relevant course or meetings.

2.2: The senior leadership Team will:

- Identify the school's Safe Guarding Leads (DSLs)
- Summarise any form of formal reporting, presented by the Online Safety Leader.
- Brief the Online Safety Leader and staff prior to formal meetings with parents, governors or inspectors.
- Provide opportunities for staff to share good practice, concerns and the arrangements for its delivery to pupils, classes and year groups.

2.3: The subject leader will:

- Keep staff updated with current Online Safety issues.
- Provide guidance and support on the implementation of the unit of work for Computing.
- Organise, review and purchase resources.
- Remain up-to-date with new developments in Online Safety.
- Monitor Online Safety throughout the school by monitoring.
- Arrange staff training.
- Liaise with colleagues in other agencies and outside agencies.
- In conjunction with Headteacher will ensure firewall is updated to block any inappropriate identified material.

2.4: The ICT manager will:

- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school.
- Ensure that schools ICT systems are secure and protected against viruses, and that such safety mechanisms are updated regularly.
- Conduct a full security check and monitor the school's ICT systems on a termly basis
- Block access to potentially dangerous sites where possible, preventing the downloading of potentially dangerous files.

2.5: The class teacher will:

- Ensure all pupils are aware of the rules for Online Safety.
- Follow the objectives as laid out in the unit of work.
- Prepare and implement teaching plans.

- Consult and work closely with the Online Safety Leader.
- Raise SLT awareness of inappropriate material identified.
- Report to the DSL any event regarding pupil accessing inappropriate material.
- Ensure that any online safety incidents are dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber bullying are dealt with appropriately in line with the school behaviour policy.

<u>2.6: Parents:</u>

The school will raise parent's awareness of Internet safety in letters or other communications home and in information via our website. This policy will also be accessible to parents. Online safety will be covered during our annual year group curriculum evenings. Parents will be invited to attend an annual online safety meeting once a year with ECP.

- Notify a member of staff or the headteacher have any concerns or queries regarding this policy.
- Ensure their child understands the four specific rules we have in place for online safety.
- Help their child to behave in a safe and respectful way, when using devices to access the Internet at home.
- Monitor take responsibility for the child's access to the Internet at home.

Teaching and Learning

3.1 Equal opportunities

At Key Stage 1 it is compulsory to teach Online Safety. Online Safety should be taught within Computing and PSHE lessons. Children should be taught to use technology safely and respectfully, keeping personal information private. They should be able to identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

As a school we are committed to the equality of opportunity to enable all individuals to achieve their full potential in Online Safety irrespective of gender, race, class, ability - intellectual or physical and sexual orientation.

We aim to achieve this by:

- Positively reflecting and building on the contributions of all children irrespective of gender, cultural background or ability, through valuing their work, praise and encouragement.
- Selecting and reviewing resources and activities carefully, to ensure equality of access.
- Positively discriminating to ensure acquisition of skills.
- Appropriately planning and differentiating both by input, support and outcome.
- Using appropriate teaching styles.
- Providing excellent role models and high teacher expectations.

3.2 Safeguarding

Any areas of concern will be raised with the DSL immediately. A culture of safeguarding is embedded in the school and the Computing leader oversees the implementation of this in the subject.
The Online Safety Leader has completed the CEOP Thinkuknow training. The Online Safety Leader will advise teachers on the importance of Online Safety during staff meetings. Staff will read and sign the 'Staff code of conduct 'during the September Inset day. All staff will complete annual safeguarding training.

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct 'before using any school computing resources. This will be signed annually during the September Inset day.
- The school will maintain a current record of all staff and pupils who are granted access to school computing systems.
- Access to the Internet will be monitored by class teachers.
- Parents will be asked to sign a consent form on Arbor.
- Any person not directly employed by the school will be supervised while accessing the school system.

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.

- The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit 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

- 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.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.
- Access to the school's complaints procedure is on 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 the school Online Safety Policy.

3.3 Inclusion

All children will learn how to stay safe when online. Children will have adult supervision at all times when using internet accessible devises. All devises have filters to allow for independence. Teachers should make themselves aware of children with additional needs who may not understand the online safety rules and ensure extra support is given depending on the activity in order to stay safe online.

3.4 External support and filtering

- The School will use ZEN (broadband provider) to ensure systems are in place to protect pupils. The school will use external training and support as needs arise.
- Surrey provide 'Net Nanny' which filters out inappropriate material.
- School Computing systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the school technology company.

3.5 Planning

Online safety has been planned for Key Stage One by the Computing Leader and is written into the Computing unit plans. Teachers should use the units of work when writing weekly plans. If other online issues arise teachers should explore these within their class. Online safety in the EYFS is not mandatory but Oatlands will continue to provide children with the knowledge they need in order to stay safe when online.

3.6 Teaching

Online safety should be taught at all times when children are accessing the internet. Discrete lessons have been planned to explore different areas of Online Safety which will be taught on a termly basis. Online safety rules are displayed in all classrooms and the commuting suite. Online safety can also be taught during PSHE lessons if issues arise. All year groups will set an online safety homework once a term. This will help to start open conversations at home about staying stay online and help to support parental engagement.

There will be an annual Online Safety assembly for all year groups provided by Education Child Protection (ECP). Teachers and LSA's to all attend.

3.7 Assessment

There is an assessment overview of the knowledge, understanding and skills that children will have achieved by the end of Year 2. Teachers need to make assessment judgements through the planning, making and evaluating process against the attainment targets in the National Curriculum. Teachers will use open-ended questions, closed questions, observations and evidence from children's work to inform assessment judgements.
Teachers in KS1 assess children against identified key skills and knowledge. These formative assessments then feed into an annual report given to parents about their child's progress in the subject and are passed to the next class teacher to support their planning.
Teachers is EYFS use Tapestry to record observations and track children's progress towards the ELGs.

3.8 Resources

Online safety posters are displayed in every classroom and the computing suite.

3.9 Monitoring

The subject leader monitors the subject in line with the school monitoring schedule. The subject leader is provided with leadership time to meet with their curriculum governor, prepare and implement annual curriculum development plans and review their policy. The subject leader will also support staff with any CPD needs and observe and monitor planning, teaching and progress to ensure the aims of the subject are being met.

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy as appropriate to age and stage.
- Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

4.1 Information system security

- School Computing systems security will be reviewed regularly.
- Virus protection will be updated regularly
- Security strategies will be discussed with the school technology company.

4.2 E-mail

Communication with staff and parents is wherever possible, electronic. To preserve school security and confidentiality the following should be observed:

- Staff and PTA community members may only correspond on school business using approved e-mail accounts.
- All teaching staff and PTA members are provided with an Oatlands email account. All should password protect and use for all school business.
- Contact with individual parents should be made only from head, info (school office), SENCo accounts or if appropriate Arbor mail.
- Contact with groups of parents can be made via Arbor mail
- All communications with parents should be authorised via head teacher or Admin prior to sending.
- Private/school email addresses should not be shared with parents.
- Group communications must always be sent BCC.
- Email communications should reflect the quality of a written communication.

4.3 Wifi

- The school is equipped with Wifi throughout. Only School devices will have access to the Oatlands Wifi.
- There is a Guest wifi.

4.4 Social Network sites

- All staff must undertake to not 'friend 'pupils, parents or family members of current or ex-pupils.
- All staff must exercise extreme caution on friending members of the community.
- All staff must recognise they have a duty of respectability and should not upload content onto sites that would compromise this duty.
- All staff must refrain from posting or viewing any content that could compromise professional integrity or bring; the school, it's reputation, the staff or pupils into disrepute.

4.5 Mobile Devices

- Pupils are prohibited from bringing mobile devices into school.
- Personal mobile phones and associated cameras will not be used during lessons or formal school time.
- Mobiles devices should be put away during teaching sessions.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where contact about pupils is required, if personal phones need to be used then 141 will be used to keep numbers confidential.
- Permission must be granted by the head teacher for any extenuating circumstances.
- Children to inform class teacher if someone takes an inappropriate photograph of them.

4.6 Published content and the school website

- The school contact details will be published on the Web site.
- The Admin Staff will take overall editorial responsibility and ensure that content is accurate, appropriate and inline with statutory DFE requirements.
- All changes will be run past the Headteacher for approval.

4.7 Publishing pupil's images and work

- Pupils images and work will be published only on secure sites e.g School website, Class Dojo, Tapestry.
- Material on the Class Dojo and Tapestry must be school related.
- Parents will be informed via Arbor, of the school policy on image taking and publishing, both on school and independent electronic repositories.
- Parents can give permission on Arbor for their child to have their photo taken.

4.8 Managing filtering

- The school will work in partnership with ZEN (broadband provider) to ensure systems are in place to protect pupils. This will be reviewed and improved regularly.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Class Teacher, the Online Safety Leader or the head teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.9 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.
- Material that would compromise professional integrity should never be downloaded onto a computer or laptop.
- Games machines including Sony Playstation, Microsoft Xbox and others that have Internet access may not be used within school.

4.10 Protecting personal data

- Personal data will be recorded processed, transferred and made available according to the Data Protection Act 1998.

Communications

5.1 Introducing the Online Safety policy to pupils

- Appropriate elements of the Online Safety policy will be shared with the pupils.
- Online Safety rules will be posted in all networked rooms.
- Curriculum opportunities to gain awareness of Online Safety issues and how best to deal with them will be provided for pupils.

5.2 Staff

- All staff will be given the School Online Safety policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Filtering systems and monitoring Computing use will be completed by senior management. Refer to the Whistle Blowing Policy.

5.3 Enlisting parental support

- Parents and carers will regularly be provided with information on Online Safety.
- The school will ask new parents to sign the parent/pupil agreement on Arbor when they register their child with the school.
- Parents will be invited to an annual Online Safety meeting provided by Education Child Protection (ECP).
- Parents to engage with a termly Online safety bookshare homework to promote open conversations at home.

Appendix 1.

Online Safety Rules

Sid's 5 top tips:
1. People you don't know are strangers. They're not always who they say they are.
2. Be nice to people on the computer like you would on the playground.
3. Keep your personal information private.
4. If you ever get that 'uh oh 'feeling, you should tell a grown up you trust.
5. If someone takes a photograph of you and you do not like it - tell a grown up.

These rules have be taken from CEOPS www.thinkuknow.co.uk

Appendix 2.

Staying Safe Online

10 top tips:
1. Don't post any personal information online – like your address, email address or mobile number.
2. Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore.
3. Keep your privacy settings as high as possible
4. Never give out your passwords
5. Don't befriend people you don't know
6. Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do
7. Remember that not everyone online is who they say they are
8. Think carefully about what you say before you post something online
9. Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude
10. If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately

These rules have been taken from www.safetykidsnet.org