Oswald Road Primary School

Online Safety Policy

Governing Body ratified this policy: September 2024

To be reviewed in 3 years: September 2027

Headteacher: Deborah Howard

Chair of Governors : Peter Martin

Oswald Road Primary School

Online Safety

CONTENTS

This policy must be read in conjunction with the school's Acceptable Use Policy.

1. Aims

At Oswald Road we aim to:

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

2. Legislation & Guidance

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

3. Roles & Responsibilities

The Governing Board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on a regular basis.
- Ensuring their own knowledge of online safety issues is up-to-date (see 'Online safety in schools and colleges: Questions from the governing board' produced by UK Council for Internet Safety, which provide guidance for school governors and trustees to help them support school leaders to keep children safe online.
- Ensuring all staff undergo safeguarding and child protection training, including online safety/cyber, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Ensure the governing board receive reports about online safety on a regular basis.
- Working with the Headteacher and ICT technicians to conduct annual light-touch reviews of this policy.
- Working with the Headteacher and governing board to update this policy on a 3 yearly basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Headteacher to conduct light-touch annual reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.

- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use of ICT Policy and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites: UK Safer Internet Centre and Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see Acceptable Use Policy).

4. Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study. From

September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools In

Key Stage 1, pupils will be taught 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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly ›

Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*

- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*

- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating Parents About Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website through our internet safety page. This policy will also be available to parents on the school website.

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. The school's Acceptable Use Agreement is available to parents who are encouraged to check their child's understanding of this document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Online safety will also be covered where necessary during parents' evenings/meetings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Online Safety & The Curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE
- Computing

Online safety teaching is always appropriate to pupils’ ages and developmental stages.
Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world

safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The DSL will be involved with the development of the school's online safety curriculum. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need. Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. If Class Teachers have concerns about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

7. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

8. Pupil's Personal Electronic Devices

Mobile phones, tablets and other personal electronic devices have become widely available and accessible to pupils. The school accepts that personal mobile phones and tablets are often given to pupils by their parents to ensure their safety and personal security, but understands that such devices pose inherent risks and may jeopardise the learning environment.

As a school, we must strike a balance between personal safety and a suitable educational setting. We understand that parents may wish for their child to carry a mobile phone for their personal safety, whilst pupils may wish to bring additional devices to school for other reasons.

Pupils are responsible for their own belongings. The school accepts no responsibility for replacing property that is lost, stolen or damaged either on school premises or travelling to and from school, and at school events. Pupils are responsible for replacing school property they lose, damage or steal, including electronic devices.

Pupils and staff should enable a personal PIN or passcode on all the devices they bring to school to protect their personal data, images and videos in the event that the device is lost, stolen or accessed by an unauthorised person.

Only pupils walking to and/or from school without an adult should have personal electronic devices on their possession or unless authorised by a member of SLT. Any pupil bringing personal electronic devices into school must make their parents aware of this. All personal electronic devices will be switched off and handed in to class teachers at the start of each day. These will be stored away and only returned to pupils as they are leaving the grounds at the end of the day. No personal electronic devices will be used or accessible during the school day.

All personal electronic devices will be used in line with our Online Safety Policy. Incidents of cyberbullying will be dealt with and reported in line with the Anti-bullying Policy and the Behaviour Policy. As part of the school's ongoing commitment to the prevention of cyberbullying, regular teaching and discussion about online safety will take place as part of PSHE and computing lessons.

Pupils are required to comply with any request to check their electronic device. Failure to do so may result in said device being confiscated. Confiscated personal electronic devices will be locked away securely in the Headteacher's office and will need to be collected by the pupil's parent. A future ban on bringing in any electronic devices may also be made.

9. Acceptable Use Of The Internet

For further information, please read the school's Acceptable Use Policy.

Where appropriate, pupils, parents, staff, governors, volunteers and visitors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

The school monitors websites visited to comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

10. Emails

For further information, please read the school's Acceptable Use Policy.

Access to and the use of emails will be managed in line with the Acceptable Use Agreement. Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site.

Staff members and will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

11. Filtering & Monitoring Online Activity

For further information, please read the school’s Acceptable Use Policy.

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Headteacher. Where appropriate, prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

School use Smoothwall filtering and monitoring services.

12. Network Security

For further information, please read the school's Acceptable Use Policy.

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians (AVA). Firewalls will be switched on at all times. ICT technicians will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in Year 1 and above will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take. Users will be required to lock access to devices and systems when they are not in use.

13. Training

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. Staff will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, briefings and staff meetings).

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

14. Responding To Issues Of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Acceptable Use and Behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

15. Monitoring Arrangements

All members of staff will log behaviour and safeguarding issues on CPOMS related to online safety.
This policy will be reviewed every 3 years by SLT. At every review, the policy will be shared with the Governing Board.

16. Links With Other Policies

This online safety policy is linked to our: ›

Acceptable Use Policy

› Child Protection and Safeguarding Policy ›

Behaviour Policy

› Staff Code of Conduct

› Data Protection Policy and Privacy Notices ›

Complaints Procedure