Online Safeguarding Policy

Rationale

We believe that the use of online services and digital tools provides powerful opportunities for collaborative learning, high levels of engagement, access to rich and current content, and support for the diverse needs of all our pupils.
At our school, online technologies are embedded throughout teaching and learning, and pupils are equipped with the knowledge and skills to engage with the digital world in a balanced, healthy, and safe way. This is achieved through both technical measures—such as automatic filtering, monitoring, and protection systems—and educational measures, including the active teaching of online safety across the curriculum, clear rules for device and internet use, regular reminders of expectations, and clear reporting and response procedures when concerns or infringements arise.
This policy should be read alongside the following policies and agreements, which together form part of our safeguarding framework:
• Computing Policy
• Child Protection and Safeguarding Policy
• PSHE / RSE Policy
• Complaints Policy
• Acceptable Use Agreements (staff, pupils, parents/carers)
• Anti-Bullying Policy
• Staff Code of Conduct
• Behaviour Policy
• Disciplinary Policy
• Remote Learning Policy

The policy has been developed in consultation with the Senior Leadership Team (SLT), the Computing Lead, staff, governors, and other relevant stakeholders.
In addition, the following statutory guidance and legislation have been taken into account:
• DfE Keeping Children Safe in Education (2025)
• DfE Teaching Online Safety in Schools (2023)
• DfE Searching, Screening and Confiscation (2022)
• DfE Data Protection in Schools (2023)
• The Data Protection Act (2018) and UK GDPR
The school also acknowledges wider frameworks such as Ofsted expectations for safeguarding and curriculum delivery, as well as best practice guidance from organisations such as the UK Safer Internet Centre and the NSPCC.

Aims

In addressing the online safety of our pupils, this policy considers four categories of risk:

Content (exposure to illegal, harmful or inappropriate material such as pornography, fake news, or extremist views);

Contact (harmful interaction with others, including grooming, targeted advertising, or adults posing as children);

Conduct (unsafe or harmful personal behaviour online, such as sharing explicit messages or cyberbullying)

Commerce (risks such as gambling, scams, phishing, or inappropriate advertising).

To mitigate these risks, the school will ensure robust technical protections such as filtering and monitoring are in place and regularly updated.
A progressive online safety curriculum will be taught from Early Years to Year 6 and reinforced across all subjects and daily practice.
Staff and governors will receive ongoing training to stay informed of emerging risks and effective safeguarding strategies.
Pupils will be consulted regularly through surveys and pupil voice activities to monitor their experiences and concerns.
Parents will be supported with advice on keeping children safe at home and managing devices responsibly.
All pupils, parents, and staff will sign and adhere to updated Acceptable Use Agreements.
Clear procedures will be in place for monitoring, reporting, and responding to online safety incidents.
Data protection measures, in line with statutory requirements, will ensure that all personal information is handled securely.

This policy applies to all members of Ouston Primary School community (including staff, students /pupils, volunteers, parents /carers, visitors) who have access to and are users of Ouston Primary School COMPUTING systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the *school/academy* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the *school/academy*, but is linked to membership of the school/academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data where appropriate. Where needed, the police will be contacted to deal with/investigate an incident rather than the school.

Ouston Primary school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Curriculum

Online safety is embedded throughout the curriculum but is addressed most explicitly through Computing, RSE and Citizenship. The school's approach is developed in line with the DfE's Teaching Online Safety in Schools guidance and the UK Council for Internet Safety's Education for a Connected World framework.

Within Computing, we use the Purple Mash 2BeSafe Online Safety Scheme of Work These units to provide pupils with the underpinning knowledge and behaviours needed to navigate the online world safely and confidently, regardless of device, platform or app.

Pupils are encouraged to apply critical thinking and develop healthy scepticism when faced with new online experiences so they can assess potential risks or pitfalls. This teaching is reinforced and extended through PSHE and RSE, ensuring online safety is addressed within the wider context of relationships, health, and personal development.

Whole-school awareness events, specialist speakers, assemblies, and day-to-day role modelling by staff further strengthen the culture of safe and responsible online behaviour.

Our online safety curriculum is tailored to pupils' ages and developmental stages, while remaining flexible to respond to emerging risks in the local and wider community. Pupils are supported to evaluate what they see online, recognise persuasion techniques, understand the difference between acceptable and unacceptable behaviours, identify risks, and seek appropriate support when needed. Teachers review and quality-check all external resources to ensure they are valid, evidence-based and age-appropriate.

When inviting external visitors, the Head teacher and DSL ensure providers are suitable, safeguarding is prioritised, and sessions are delivered with sensitivity to pupils who may have lived experience of online harm.

Lessons and activities are planned to avoid drawing attention to individual pupils' circumstances, and staff follow safeguarding procedures if concerns arise during teaching.

Resources

The school uses a range of technology resources to access the internet, including desktop computers, laptops, and tablets. All resources are managed to ensure safe, reliable, and age-appropriate use.

To protect users and content, the following safeguards are in place:

• Robust content filtering appropriate to pupil age and needs, regularly reviewed by the IT network manager and overseen by the head teacher and DSL. Filtering is designed to balance safeguarding with educational access, avoiding unnecessary over-blocking.

• Security features such as regularly updated anti-virus software, firewalls, and protection against unauthorised installation of software, supported by administrative controls.

• Staff responsibility for evaluating all websites and online tools prior to classroom use. Staff also adhere to copyright law and licensing requirements when creating and using digital content.

• Access to technology and the internet is only granted once pupils, staff, and parents (where appropriate) have signed the school's Acceptable Use Agreement.

• Pupils use the internet under supervision and with clear direction to ensure purposeful, safe use.
• Incidents of inappropriate content are reported immediately to the IT network manager, who investigates, and any changes to filtering are authorised by the head teacher in consultation with the DSL.
• Breaches of filtering systems are managed under the behaviour policy (for pupils) or the disciplinary policy (for staff). Suspected access to illegal material is immediately reported to the police or CEOP.
• The DSL manages cases relating to misuse or failures of filtering and ensures safeguarding processes are followed.
• All network users have unique usernames and passwords, which must be kept private. Staff are required to change their passwords every six months. Devices must be locked when unattended to prevent unauthorised access.
Additional measures include regular audits of technology resources, reporting systems for staff to raise issues promptly, and provision of staff training to ensure consistent understanding of safe and effective use of resources. The school also plans strategically for replacement, upgrades, and accessibility, ensuring resources meet the needs of all learners, including those with SEND

Inclusion

Our aim is to ensure that all pupils develop a secure understanding of how to protect their own and others' safety online, regardless of ability, background, or circumstance. This includes children with special educational needs and disabilities (SEND), those with English as an additional language (EAL), pupils from different social and cultural backgrounds, and other vulnerable groups.
We recognise the vital role technology plays in enabling access to learning for all pupils. For those with SEND or disabilities, technology can provide flexible, personalised support that removes barriers and enhances independence. To this end, we ensure that additional access to devices and assistive technologies is available during the school day and, where appropriate, beyond school hours.
The school acknowledges that while every child may be at risk online, some pupils face greater vulnerabilities. For example, looked-after children (LAC), pupils with limited family support, or those with particular communication needs may require tailored approaches to online safety. Staff working closely with these pupils—such as the SENCO, designated teacher for LAC, and DSL—collaborate to adapt the curriculum and support provision. This ensures that all children not only receive equitable access to technology but also develop the resilience, knowledge, and strategies needed to stay safe online.
Staff are trained to identify barriers to inclusion in online safety education and to differentiate teaching approaches accordingly. Online safety messages are delivered in accessible formats—for example, simplified language, visual aids, or practical modelling— to ensure all pupils can engage meaningfully.

Roles and Responsibilities

Online safety is the responsibility of the whole school community.

The **governing body** ensures that online safety is embedded as a safeguarding priority, holding leaders to account for policy, provision, and resourcing.

The **head teacher** provides overall leadership, creating a culture that values safe and responsible online behaviour and ensuring policies are consistently implemented.

The **Designated Safeguarding Lead** (DSL) has day-to-day responsibility for online safety within the safeguarding framework, ensuring staff and pupils know how to report concerns, recording incidents, and leading curriculum integration.

The **IT Network Techncian** oversees the security and reliability of the school's digital infrastructure, including filtering, monitoring, and technical protections, while also advising on safe procurement and supporting incident response.

All staff are responsible for modelling and teaching safe online behaviour, embedding online safety into their practice, and reporting concerns promptly.

Pupils must follow the school's Acceptable Use Agreement, demonstrate respect and responsibility online, report concerns to trusted adults, and use technology in a way that supports learning while protecting themselves and others.

Exit strategy

- At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Monitoring

The school is committed to robust monitoring of online safety provision to ensure that pupils are safe, staff are confident in their roles, and policies are consistently applied. Monitoring is achieved through a range of strategies including observations, pupil and staff voice, learning walks, work scrutiny, reflective teacher feedback, and ongoing checks of the learning environment.
Dedicated leadership time is allocated to ensure these activities are purposeful and sustained.
Evaluation and feedback are essential for continuous improvement.
Leaders use recognised national standards and frameworks to benchmark practice and identify areas for development.
Whole-school priorities relating to online safety are shared and discussed during staff training, staff meetings, and through dedicated CPD opportunities. This ensures that all staff remain informed and accountable for maintaining high standards of online safety.
Clear reporting structures are in place. Concerns regarding staff online behaviour are reported directly to the head teacher in line with the Staff Code of Conduct and Disciplinary Policy.
Concerns regarding pupil online behaviour are reported to the Designated Safeguarding Lead

(DSL), who investigates in line with the Child Protection and Safeguarding Policy and Behaviour Policy, with support from the head teacher and IT Network Manager if required. The DSL records and tracks all online safety incidents, ensuring that patterns and recurring issues are identified, addressed, and reported to senior leadership and governors as appropriate.
Monitoring processes also ensure that filtering and security systems are reviewed regularly, with feedback from staff and pupils feeding into ongoing evaluation of their effectiveness. Leaders use this evidence to inform improvements, resource allocation, and training needs, ensuring the approach remains responsive to evolving risks.

Communication

The policy will be communicated to staff/pupils/community in the following ways:
- Policy to be posted on the school website and posted in the staffroom.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use policy discussed with staff and pupils at the start of each year. Acceptable use policy to be issued to whole school community, on entry to the school.

Staff and governor training

All staff and governors receive safeguarding and child protection training, which includes online safety, as part of their induction and is repeated following the school's training review programme. This ensures that from the outset, every member of staff and governor understands their responsibilities for keeping pupils safe online and continue to do so. Regular updates on online safety are provided at least annually, and more frequently if emerging risks or national/local guidance require.
The Designated Safeguarding Lead (DSL) and deputies undertake accredited safeguarding training that is refreshed at least every two years, with specific content covering online safety. In addition, they receive regular briefings and updates on online risks, evolving technologies, and best practice, enabling them to act as key sources of expertise within the school. All staff are trained and reminded about the correct procedures for reporting online safety concerns in line with the school's safeguarding, behaviour, and disciplinary policies.
Training also emphasises the importance of modelling safe and responsible online behaviours, understanding the different vulnerabilities of pupils (including those with SEND, EAL, and LAC), and using curriculum opportunities to reinforce online safety messages. Where appropriate, staff are encouraged to attend specialist CPD opportunities, including those offered by the local authority, multi-academy trust (if relevant), or national providers. Leaders evaluate the impact of training by reviewing staff confidence, monitoring incidents, and ensuring staff are able to apply training in day-to-day teaching and safeguarding practice. Governors are updated on staff training as part of safeguarding reports to ensure accountability.
Staff and governors complete Cyber Security training annually also.

Parent/Carer awareness and training

The school works in close partnership with parents and carers to ensure pupils are supported both at school and at home to stay safe online.
Parents play a vital role in reinforcing the messages pupils receive in school and in providing a trusted support network if concerns arise.
When pupils join the school, parents and carers are given a copy of the Acceptable Use Agreement to review and sign with their child. This ensures shared understanding and commitment to safe and responsible technology use. The school provides regular opportunities for parents to access up-to-date guidance on online safety. This includes dedicated time at parents' evenings, termly newsletters, website updates, and signposting to high-quality online resources.
The school also shares information in response to emerging risks or trends, such as new apps, games, or scams. Workshops or information sessions may be offered, led by school staff, external specialists, or local safeguarding professionals. These sessions are designed to provide parents with practical strategies for managing technology use at home, setting boundaries, and having open conversations with their children about online behaviour.
The school values parent/carer feedback and seeks their views through surveys and informal discussions to ensure the support offered is relevant, accessible, and responsive to the needs of the community.

Expectations in school

Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the ICT safety acceptable use agreement form.
- Should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

E-mail

Our school:

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of staff on the school website. We use anonymous or group e-mail address, for example info@oustonprimary.org.uk for communication with the wider public.
- Any apps educational or Classroom management (Class Dojo) used by school are GDPR compliant.

• 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.
• Will ensure that email accounts are maintained and up to date.
• We use systems in the school, including desktop anti-virus products, plus direct email filtering for viruses.

Pupils:
• Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home

Staff:
• Staff can only use approved Ouston Primary School e- mail systems on the school system. • Staff will use the approved Ouston Primary School e-mail systems for professional purposes.
• Access in school to external personal e-mail accounts may be blocked.
• Never use email to transfer staff or pupil personal data. 'Protect-level' data should never 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.

School website

• The Head teacher, 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. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Cloud Environments

• Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
• Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.
• In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors:
• Staff are instructed to always keep professional and private communication separate.
• Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
• The use of any school approved social networking will adhere to school's online and computing policy.

School staff will ensure that in private use:
• No reference should be made in social media to pupils, parents/carers or school staff.
• School staff should not be online 'friends' with any pupils. Any exceptions must be approved by the Head teacher.

- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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 online school rules.

Parents:
- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they are not permitted to upload photographs, videos or any other information about other people.

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.

Data security: Management Information System access and Data transfer Strategic and operational practices

At our school:
- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- We require staff to log-out of systems when leaving their computer.
- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- 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 devices.

- No pupil within years Nursery to Year 4 should bring his or her mobile phone or personally-owned device into school (unless given permission from the Head teacher) Any device brought into school will be confiscated and returned at the end of the school day. Pupils within year 5 and 6 may bring their mobile devices into school having completed a school permission letter. Mobile phones must be handed to the class teacher on entry to the school to be kept securely locked away within the school office. No mobile phone is allowed to be used on the school premises by a pupil.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Head teacher.
- Pupil personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned. Parents/carers should not take photos/videos during school events.
- Staff members may use their phones during lunch times but only within non-child areas, E.g. the staff room,
- All visitors are requested to keep their phones on silent and must not use their devices in school
- If a pupil needs to contact his or her parents or carers, the phone in the school office will be used and supervised by a staff member.
- If a staff member is expecting a necessary/urgent personal call they may leave their phone with the school office to answer on their behalf or ask for the call to be made to the school office.
- Mobile phones/smart watches/tablets/MP3 players should not be brought into school. The school takes no responsibility for loss or damage of any personal devices brought to school.

Digital images and video

In our school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Protecting personal data

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

The Online Safety Policy will be reviewed at least annually, and sooner if there are significant changes in statutory guidance, safeguarding expectations, technology, or local risk (e.g., emerging online harms, platform updates, or incident trends). Interim updates may be issued by the head teacher and DSL following consultation with the governing body to ensure alignment with Keeping Children Safe in Education, data protection requirements, and the school's wider safeguarding and curriculum policies. staff, pupils, and parents/carers. Each review will draw on incident logs, monitoring reports, pupil and parent voice, staff feedback, and technical audits (filtering/monitoring), with outcomes communicated to iPad and Laptop usage policy

Review date: April 2027