# Online E-Safety Policy

2023/2024

| | |
|---|---|
| Ownership | Ajla Duckollari |
| Date Created | March 2023 |
| Reviewed | March 2024 |
| Next Review | March 2025 |

Key Contact

| | |
|---|---|
| Ajla Duckollari (Principal) | principal@oxfordonlineschool.org |
| Avery Jayne Benton (Head of Academics) | a.benton@oxfordonlineschool.org |

## INTRODUCTION

At Oxford Online School, digital technology serves as a crucial tool for facilitating learning. The internet, along with other digital and information technologies, not only provides students with valuable learning opportunities but also plays a significant role in their daily lives, allowing them to connect and collaborate with fellow students.

While Oxford Online School advocates for the integration of digital technology across the curriculum, we also recognize the importance of ensuring safe internet access and responsible use. It is vital that students are empowered to build resilience and develop strategies to prevent, manage, and respond to online risks. Our commitment to fostering a safe, positive, and inclusive online learning environment aligns with the Department for Education's guidelines in *Keeping Children Safe in Education (2024)* and *Teaching Online Safety in Schools (2023)*.

## PURPOSE OF THIS POLICY

The purpose of this policy is to ensure the appropriate and safe use of the internet and other digital technology devices by all members of the Oxford Online School community.

This policy aims to:

- Safeguard and protect all members of the school community online.
- Outline strategies to educate and raise awareness about online safety throughout the community.
- Enable staff to work safely and responsibly, model positive online behavior, and uphold professional standards when using technology.
- Establish clear procedures for responding to online safety concerns.

## THE FOUR KEY CATEGORIES OF RISK

At Oxford Online School, our approach to online safety focuses on addressing four key categories of risk:

1. **Content** – Exposure to illegal, inappropriate, or harmful material, including but not limited to pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalization, and extremism.
2. **Contact** – The dangers of harmful interactions online, such as peer pressure, targeted commercial advertising, and encounters with adults who pose as children or young adults with the intent to groom, exploit, or abuse them for sexual, criminal, financial, or other purposes.
3. **Conduct** – Online behaviors that increase the risk of harm or directly cause it, such as the creation, distribution, or receipt of explicit images (including consensual and non-consensual sharing of nudes, semi-nudes, and pornography), sharing other inappropriate content, and engaging in cyberbullying.
4. **Commerce** – Risks associated with online financial activities, including online gambling, exposure to inappropriate advertising, phishing schemes, and other financial scams.

## RESPONSIBILITIES

### LEADERSHIP TEAM

The Principal at Oxford Online School is responsible for ensuring that all staff fully understand this policy and consistently implement it across the school. The Principal also oversees regular audits and evaluations of online safety practices to identify both strengths and areas needing improvement.

Details of the school's Designated Safeguarding Lead (DSL) and deputies are outlined in our child protection and safeguarding policy, as well as in relevant job descriptions.

The DSL has primary responsibility for online safety within the school, specifically:

- Assisting the Principal in ensuring that all staff are well-versed in this policy and that it is consistently applied throughout the school.
- Collaborating with the Principal, Head of Academics, and other staff members as needed to address any online safety issues or incidents.
- Managing all online safety concerns and incidents in accordance with the school's child protection policy.
- Ensuring that any online safety incidents are recorded as concerns in Managebac and handled appropriately in line with this policy.
- Logging and appropriately addressing any incidents of cyberbullying in accordance with the school's behavior and anti-bullying policies.
- Providing updates and delivering staff training on online safety, often as part of broader safeguarding training.
- Liaising with external agencies and services when necessary.
- Regularly reporting on online safety issues to the Principal.
- Implementing and regularly reviewing security measures such as filtering and monitoring systems to protect students from harmful and inappropriate online content, including terrorist and extremist material, while using the school's online platforms such as Managebac, Zoom, Google Shared Drive, and Google Classroom. Only teachers are permitted to publish content on these platforms.
- Supporting parents' understanding of online safety through initiatives such as our NSPCC Parent Workshops.

**STAFF**

All staff at Oxford Online School are responsible for:

- Maintaining a thorough understanding of this policy.
- Consistently implementing this policy in their daily activities.
- Agreeing to and adhering to the acceptable use of the school's platforms, including Managebac, Zoom, Google Classroom, and Google Shared Drive.
- Collaborating with the DSL to ensure that any online safety incidents are logged in Managebac and appropriately managed in accordance with this policy.
- Ensuring that any incidents of cyberbullying are addressed in line with the school's behavior policy.
- Responding appropriately to all reports and concerns related to sexual violence and/or harassment, both online and offline, while maintaining an attitude of 'it could happen here

**PARENTS**

Parents at Oxford Online School are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms of acceptable use of the school's ICT systems and internet.
- Support the school's online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviors at home.
- Ensure their own home network and systems have a high level of security protection.
- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children.
- Identify changes in behavior that could indicate their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risks or concerns online.
- Use school systems, such as learning platforms like Managebac and Google Classroom, as well as other network resources, safely and appropriately.
- Take responsibility for staying informed about the risks and opportunities posed by new and emerging technologies.

Parents can seek further guidance on keeping children safe online from the following organizations and websites:

- [What are the issues? – UK Safer Internet Centre]
- [Current topics – Childnet International]
- [Parent resource sheet – Childnet International]

## PUPILS

*(At a level that is appropriate to their individual age, ability, and vulnerabilities)*

Pupils at Oxford Online School are expected to:

- Participate in online safety education opportunities that are appropriate for their age and ability.
- Read and adhere to the school's Acceptable Use Agreements.
- Respect the feelings and rights of others both online and offline, whether in or out of school.
- Take responsibility for keeping themselves and others safe online.
- Report any concerns they encounter online to a trusted adult.

## EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils at Oxford Online School will receive education on online safety as part of the Wellbeing curriculum. By the end of the program, pupils will be equipped with knowledge and skills to navigate the online world safely and responsibly. They will learn:

- Their rights, responsibilities, and opportunities in the online environment, with the understanding that the same standards of behavior apply both online and offline.
- The risks associated with online activities, including the fact that anything shared online can potentially be redistributed and that it is difficult to remove compromising material once it is posted.
- The importance of not sharing content that they would not want widely distributed and the necessity of not sharing personal material that is sent to them by others.
- How to seek support and report concerning material or issues they encounter online.
- The potential harm of viewing inappropriate content.
- The dangers of sexually explicit material (e.g., pornography), including how it distorts perceptions of sexual behavior, affects self-image, and negatively influences interactions with sexual partners.
- The legal implications and severe penalties, including imprisonment, associated with sharing or viewing indecent images of children, including those created by minors.
- How data and information are generated, collected, shared, and used online.
- How to recognize harmful behaviors online, such as bullying, abuse, or harassment, and where to report these behaviors or seek support if affected.
- How to understand and communicate consent, including sexual consent, and the importance of recognizing when and how consent can be withdrawn in any context, including online.

Additionally, pupils will be supported in building resilience against radicalization by providing a safe space for discussing controversial issues and learning how to actively participate in and influence decision-making processes.

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

**LEARNING ONLINE**

Oxford Online School utilizes Managebac, Google Classroom, Zoom, and Google Meet as its primary online learning platforms. The Senior Leadership Team and teachers consistently monitor the use of these platforms in their daily operations, including the use of messaging features and discussion forums. Access to these platforms is restricted to current members of staff, pupils, and parents.

For delivering live and recorded lessons, Oxford Online School uses Zoom and Google Meet. Only authenticated users are permitted to join live classes.

- **Teacher Control**: Teachers manage entry to live classes via the waiting room feature in Zoom and Google Meet.
- **Visibility**: Teachers are always visible on webcam, in accordance with the school's teacher standards and expectations policy.
- **Engagement**: The use of cameras and microphones is encouraged to foster a sense of community within the classrooms. Pupils have the flexibility to engage in online lessons in various ways: using the chat box only, verbally and with the chat box, the chat box and webcam, or verbally with both the chat box and webcam. These options are designed to accommodate the diverse needs of pupils.
- **Teacher Controls**: Teachers have the ability to turn off webcams and microphones for individual pupils or the entire class as needed. They also control who can share their screen and annotate documents or images during lessons.
- **Communication**: Pupils can communicate with the teacher publicly using the chat function in Managebac, Zoom, Google Meet or privately via email during live lessons.
- **Administrative Access**: Only key administrators are granted access to Google admin control functions.
- **Security**: The unique login and password details for accessing school platforms must be kept securely to prevent unauthorized access.

By enrolling at Oxford Online School, parents and carers consent to their child or young person participating in video conferencing via Zoom and Google Meet, including the use of chat, webcam, and microphone functions.

### Camera Expectations

At Oxford Online School, our expectation is that all teachers will use their webcams while delivering lessons online, and we also encourage students to use their webcams during lessons. There are numerous benefits to students using webcams during lessons, including:

- **Enhanced Sense of Community**: Webcams help students feel more connected to their peers and the learning environment.
- **Visual Cues**: Teachers can better interpret visual cues, such as recognizing when a student is struggling and needs assistance.
- **Immediate Feedback**: Students can quickly show their work, allowing teachers to provide immediate feedback or address any misconceptions during the live lesson, rather than waiting for an uploaded assignment.

To ensure the safety and appropriateness of webcam use during lessons, all teachers and students are required to adhere to the following guidelines:

- **Appropriate Attire**: Users should be dressed suitably for a learning environment.
- **Consideration of Background**: Users should be mindful of what is visible in the webcam background, such as wall displays or personal items.
- **No Unintended Participants**: Other individuals, such as parents or siblings, should not be visible on the webcam during lessons.

### Live Lessons

Oxford Online School ensures that lesson recordings are accessible only to students enrolled in that particular class, their teachers, and the Principal. All live lessons are recorded and securely stored for potential academic or safeguarding reviews.

- **Appropriate Location**: Computers and laptops should be positioned in an appropriate setting for learning.
- **Professional Language**: Language used during lessons, including by any family members or friends in the background, should be appropriate and professional.
- **Microphone Etiquette**: When not speaking, users should keep their microphones muted to minimize background noise.
- **Respectful Participation**: To contribute to discussions, students should avoid talking over others. They can use the 'raise hand' function and wait to be called upon by the teacher or for a natural pause in the conversation.

If there is a specific reason why a student feels uncomfortable appearing on webcam during lessons, parents or students are encouraged to contact their mentor or Head of Year to discuss their concerns.

### Categories of Lesson Contribution

Students can engage in online lessons through three different categories of participation:

1. **Text-Based Contribution**: Participate via text chat, collaborate by writing on shared documents and whiteboards, and share work without using a microphone or camera.
2. **Text and Audio Contribution**: Engage via text chat, collaborate on shared documents and whiteboards, share work, and contribute verbally using a microphone.
3. **Full Participation**: Engage via text chat, collaborate on shared documents and whiteboards, share work, contribute verbally using a microphone, and appear on camera.

## COMMUNICATION AND SOCIAL MEDIA

### Expectations

All digital communication between staff and students or parents/carers at Oxford Online School must be professional in tone and content. Under no circumstances may staff use personal email addresses, mobile or landline phone numbers, or social media to contact a student or parent/carer. The school provides staff with access to their work email addresses at all times for use in school-related communications.

The term "social media" includes, but is not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms, and instant messaging platforms. All members of the school community are expected to engage with social media in a positive, safe, and responsible manner at all times.

### Staff Communication and Use of Social Media

- The safe and responsible use of social networking, social media, and personal publishing sites is discussed with all staff members during their induction and is regularly reinforced through ongoing staff training.
- Professional and safe behavior on social media is outlined for all staff members as part of the staff Code of Conduct and the Acceptable Use Agreement.
- Staff must not access social networking sites, personal email, or any unrelated websites while teaching or in the presence of students.
- When using social networking sites, staff must exercise extreme caution, being mindful of the content they publish online and its potential impact on their professional standing and the reputation of the school.
- The school has implemented measures to ensure that the school's digital platforms are secure. Staff should be aware that all communications made through the school's platform and staff email addresses are monitored.
- Any communication that makes staff feel uncomfortable or that is offensive, discriminatory, threatening, or bullying in nature must be immediately reported to the DSL. Staff should not respond to such communications.

- Staff must remain vigilant about the risk of fraudulent emails and report any suspicious emails to the appropriate school authority.
- Any online communications, whether conducted on school or personal devices, must not knowingly or recklessly:
    - Place a child or young person at risk of harm, or cause actual harm.
    - Bring the school into disrepute.
    - Breach confidentiality or data protection legislation.
    - Violate copyright laws.
    - Engage in behavior that could be considered discriminatory, bullying, or harassing, including making offensive or derogatory comments related to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief, or age; bullying another individual through social media; or posting links to or endorsing material that is discriminatory or offensive.

## PHISHING & SPAM

### Advice for Parents / Carers

- **Educate Your Children**: It's essential to teach your children about the dangers of phishing and spam emails. Make sure they understand that they should never click on links or open attachments from unknown senders.
- **Monitor Email Activity**: Regularly check your children's email accounts to ensure they are not receiving or responding to suspicious messages.
- **Use Strong, Unique Passwords**: Encourage your children to use strong, unique passwords for their email and online learning accounts to prevent unauthorized access.
- **Enable Two-Factor Authentication (2FA)**: If available, enable two-factor authentication on your children's accounts to add an extra layer of security.
- **Install Security Software**: Ensure that all devices used for online learning have up-to-date antivirus and anti-malware software installed.
- **Report Suspicious Emails**: Teach your children to report any suspicious emails to you or their teachers immediately.

If you have concerns about suspicious emails, please contact the Head of Operations.
For more information, view Appendix 1 for useful links and resources.

### Advice for Staff

- **Stay Informed**: Keep up to date with the latest phishing and spam tactics to recognize and avoid them effectively.
- **Verify Sender Information**: Always verify the sender's information before clicking on links or downloading attachments from emails, especially if the email is unexpected.
- **Use Official Channels**: Communicate with students and parents through official school channels and platforms to reduce the risk of phishing attempts.

- **Regular Training**: Participate in regular training sessions on cybersecurity to stay aware of new threats and how to handle them.
- **Strong Passwords and 2FA**: Use strong, unique passwords for all school-related accounts and enable two-factor authentication wherever possible.
- **Report and Escalate**: If you receive a suspicious email, report it to the Head of Operations immediately and do not engage with the content.
- **Security Software**: Ensure all your devices have the latest antivirus and anti-malware software installed and updated regularly.
- **Be Cautious with Personal Information**: Never share personal or sensitive information through email, especially if the request seems unusual or urgent.

## CYBER-BULLYING

### Understanding Cyber-Bullying

Cyber-bullying occurs online, often through social networking sites, messaging apps, or gaming platforms. Like other forms of bullying, it involves the repetitive, intentional harm of one person or group by another, where there is an imbalance of power. (Refer to the school behaviour policy for more details.)

### Preventing and Addressing Cyber-Bullying

To prevent cyber-bullying, we will ensure that pupils understand what it is and how to respond if they experience or witness it. Pupils will be informed about the reporting process and encouraged to report incidents, whether they are victims or witnesses.

The school will actively engage students in discussions about cyber-bullying, including its causes, various forms, and potential consequences. These discussions will occur in mentor sessions and assemblies, whether for the whole school or specific year groups.

Teaching staff are encouraged to incorporate lessons on cyber-bullying into the curriculum whenever possible. Additionally, the school has created a dedicated parent guide webpage to provide support and resources.

In the event of a specific incident of cyber-bullying, the school will follow the procedures outlined in the school behaviour policy. If illegal, inappropriate, or harmful material has been disseminated among pupils, the school will take all reasonable steps to contain the incident.

If the Designated Safeguarding Lead (DSL) has reasonable grounds to believe that the material in question is illegal, they will report the incident and provide relevant materials to the police as soon as practicable. The school will also collaborate with external services if necessary.

## ACCEPTABLE USE OF THE INTERNET AND SCHOOL SYSTEMS

All pupils, parents, staff, volunteers, and governors are required to sign an agreement regarding the acceptable use of the school's ICT systems.

The use of the school's systems, including ManageBac, must be strictly for educational purposes or for fulfilling the duties associated with an individual's role within the school.

## HOW THE SCHOOL WILL RESPOND TO MISUSE OF ITS SYSTEMS

If a pupil misuses the school's ICT systems or the internet, the school will follow the procedures outlined in its policies on behaviour and acceptable use. The response will be proportionate to the individual circumstances, nature, and seriousness of the specific incident.

If a staff member misuses the school's ICT systems or misuses a personal device in a manner that constitutes misconduct, the situation will be addressed in accordance with the staff code of conduct. The action taken will be based on the specific circumstances, nature, and seriousness of the incident.

The school will assess whether incidents involving illegal activity, inappropriate content, or other serious breaches should be reported to the police.

## TRAINING

All staff members will receive training as part of their induction, covering safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalization.

Additionally, all staff members will participate in refresher training at least once each academic year as part of safeguarding training. They will also receive relevant updates as needed, through channels such as emails, e-bulletins, and staff meetings.

Through this training, all staff will be made aware that:

- **Technology plays a significant role** in many safeguarding and wellbeing issues, and children are at risk of online abuse.
- **Children can abuse their peers online** through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially within chat groups.
    - Sharing abusive images and pornography with those who do not wish to receive such content.
    - Physical abuse, sexual violence, and initiation/hazing-type violence, all of which can include an online element.

The training will also help staff:

- Develop better awareness to assist in identifying the signs and symptoms of online abuse.
- Enhance their ability to ensure pupils can recognize dangers and risks in online activities and can make informed decisions about these risks.
- Strengthen their capacity to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The Designated Safeguarding Lead (DSL) and Deputies will undergo child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on online safety regularly, and at least annually.

## MANAGEMENT OF DATABASES

**Storing Pupil Data and Records (Open Apply and ManageBac)**

Oxford Online School uses Open Apply for managing student applications and enrollment data, and ManageBac for storing academic records, tracking academic progress, and maintaining pastoral notes. These platforms also facilitate communication with parents and carers.

The Operational Leadership Team is responsible for maintaining the information held on pupils, both enrolled and unenrolled. Open Apply and ManageBac are used by Oxford Online School in full compliance with data protection legislation, including GDPR.

**To ensure pupil data is protected:**

- **Access Control**: Only authorized members of the Oxford Online School team will have access to the information held on pupils within Open Apply and ManageBac.
- **Role-Based Access**: Authorized users of Open Apply and ManageBac will only be provided with the information necessary for them to perform their day-to-day duties.
- **Two-Factor Authentication**: All staff members will utilize two-factor authentication to access both Open Apply and ManageBac platforms, ensuring an additional layer of security.
- **Security Awareness**: All staff will be trained on appropriate safety measures, including the use of strong passwords, the importance of not sharing passwords, and the necessity of locking or logging out of the system when not in use.
- **Parent Portal Security**: Parents and carers will be informed of the expectations regarding the use of the Parent Portal, which operates on these platforms. This includes the use of strong passwords, not sharing passwords, and logging out of the portal when not in use.

Appendix 1

## ACCEPTABLE USE OF OXFORD ONLINE SCHOOL SYSTEMS & PLATFORMS

### Agreement for Parents and Carers

Online channels play a crucial role in how parents and carers communicate with, or about, our school. To ensure a positive and respectful environment, the following guidelines apply to the use of these channels:

**The school uses the following channels:**

- **Our official Facebook page**
- **Email/text groups for parents** (used for school announcements and information)
- **Our virtual learning platform**

Parents and carers may also establish independent channels to stay informed about what's happening in their child's class. This primarily occurs on Classlist, ensuring that private contact details do not need to be shared.

**When communicating with the school via official channels, or using private/independent channels to discuss the school, I will:**

- **Be respectful** towards members of staff and the school at all times.
- **Be respectful** of other parents, carers, and children.
- **Direct any complaints or concerns** through the school's official channels so they can be addressed in line with the school's complaints procedure.

**I will not:**

- **Use private groups, the school's Facebook page, or personal social media** to complain about or criticize members of staff. This is not constructive, and the school cannot address or improve issues unless they are raised through the proper channels.
- **Use private groups, the school's Facebook page, or personal social media** to complain about or attempt to resolve behavior issues involving other pupils. I will contact the school and speak to the appropriate member of staff if I am aware of a specific behavior issue or incident.
- **Upload or share photos or videos on social media** of any child other than my own unless I have obtained permission from the other children's parents or carers.

**By enrolling your child at Oxford Online School, you agree to these terms.**

Appendix 2

## ACCEPTABLE USE OF THE SCHOOL’S ICT FACILITIES, SYSTEMS & PLATFORMS

### Agreement for Students

When using the school’s ICT systems and platforms, I will not:

- **Use them for non-educational purposes.**
- **Use them to break school rules.**
- **Access any inappropriate websites.**
- **Access social networking sites** (unless my teacher has expressly allowed this as part of a learning activity).
- **Use chat rooms.**
- **Open any attachments in emails** or follow any links in emails sent by an external source, unless advised by my teacher.
- **Use any inappropriate language** when communicating online, including in emails, live lesson chats, and messages on ManageBac, Zoom, Google Classroom, or Google Meet.
- **Share any semi-nude or nude images, videos, or live streams**, even if I have the consent of the person or people in the photo/video.
- **Share my password with others** or log in to the school’s network using someone else’s details.
- **Bully other people**.
- **Use AI tools and generative chatbots (such as ChatGPT or Google Gemini):**
  - During assessments, including internal and external assessments, and coursework.
  - To present AI-generated text or imagery as my own work.

**I understand that the school can monitor my access to Oxford Online School platforms and systems.**

- **I will immediately inform a teacher or another member of staff** if I find any material that might upset, distress, or harm me or others.
- **I will always use the school’s ICT systems and platforms responsibly.**
- **I understand that the school can discipline me** if I engage in certain unacceptable behaviors online, even if I am not in school when I do them.

**By being enrolled at Oxford Online School, you agree to follow the rules above.**