

The Online School UK



Online Safety Policy 2026-2027

Date of This Review	August 2026
Reviewed By	Gemma Wheelwright- Rhodes and Effie Haywood
Date Approved by School Director	1st September 2026
Date of Next Review	July/ August 2027

Table of Contents

1. Introduction
2. Aims and Scope
3. Roles and Responsibilities
4. Education and Curriculum
5. Online Learning and Live Lessons, including cameras, microphones and lesson conduct
6. Communication and Professional Boundaries
7. Acceptable and Unacceptable Use
8. Artificial Intelligence and Generative AI
9. Cyber Security
10. Social Media
11. Online Bullying, Harassment and Harmful Behaviour
12. Filtering and Monitoring
13. Data Protection and Privacy
14. Online Safety Incidents and Reporting
15. Staff Training
16. Supporting Parents and Carers
17. Accessibility/ Vulnerable Students
18. Monitor, Review and Evaluation

1. Introduction

The Online School UK aims to ensure that every student and staff member in its care is safe, both online and physically. Information and communications technology (ICT) is an integral part of the way The Online School UK works and is a critical resource for all members of the school community. As an online school, technology is fundamental to teaching and learning, safeguarding, pastoral care, communication and the administrative functions of the school.

The Online School UK recognises that technology and online activity provides extensive opportunities for alternative learning pathways, alongside traditional methods. As well as for communication and professional benefits However, they also pose more significant risks to pupils, staff and other members of the school community.

These risks may include exposure to harmful or inappropriate content, harmful contact or communication, online bullying and harassment, exploitation, grooming, sexual abuse, radicalisation and extremism, misinformation and disinformation, financial scams, cybercrime, breaches of privacy and data protection, and other forms of online harm.

The school therefore seeks to promote a culture for both students and staff, in which technology is used safely, responsibly and respectfully. This policy applies to all members of the school community, including staff, students, parents, and visitors, who have access to and are users of the school's online systems and equipment.

This policy sets out the school's approach to:

- online safety
- safeguarding pupils from online harm
- the safe and responsible use of technology
- acceptable and unacceptable use of the school's ICT facilities and platforms
- filtering and monitoring
- online learning and live lessons
- communication and social media
- artificial intelligence and generative AI
- cyber security
- data protection and privacy
- staff use of technology including acceptable use
- pupil use of technology
- responding to online safety concerns and incidents

The school recognises that online safety risks can arise both through school-provided systems and through technology, platforms and devices used outside school where those activities affect the welfare, safety or education of pupils or the wider school community.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction, and leisure activities.

This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements of the policy.

Although it is exciting and beneficial both within and outside the context of education, a lot of educational technology, particularly online resources, is not policed consistently. All users need to be aware of the range of risks associated with the use of the Internet and other types of technology.

Online safety is considered an integral part of the school's wider safeguarding arrangements and is not treated as a separate or purely technical issue.

Legal Framework and Guidance

This policy has regard to relevant legislation, statutory guidance and national guidance, including:

- Equality Act 2010
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Human Rights Act 1998
- Education Act 2011
- Education and Inspections Act 2006
- Freedom of Information Act 2000
- Keeping Children Safe in Education 2026
- Searching, Screening and Confiscation guidance
- Department for Education filtering and monitoring standards
- Department for Education guidance on remote education and safeguarding
- Department for Education guidance on generative artificial intelligence in education
- Department for Education Generative AI Product Safety Standards
- National Cyber Security Centre guidance concerning cyber security in schools
- UK Council for Internet Safety guidance concerning online safety and the sharing of nude and semi-nude images
- relevant Department for Education guidance concerning relationships, sex and health education
- Prevent-related statutory guidance, where applicable
- other relevant statutory guidance and national guidance as updated from time to time

The school will review this policy regularly to ensure that references to legislation, statutory guidance and national guidance remain current.

KCSIE 2026 states that online safety should be a running and interrelated theme within the school's whole-school safeguarding approach and related policies and procedures. It also identifies the four areas of content, contact, conduct and commerce as a basis for an effective online safety policy. All of which The Online School UK follows.

2. Aims and Scope

The Online School UK aims to:

1. provide a safe online environment for pupils, staff and other members of the school community;
2. protect pupils from online harm, including harmful content, contact, conduct and commerce;
3. provide pupils with the knowledge, skills and resilience to use technology safely and responsibly;
4. ensure that online safety forms part of the school's whole-school safeguarding approach;
5. establish clear expectations for the acceptable use of school ICT facilities and platforms;
6. ensure that staff understand their safeguarding responsibilities in relation to online safety;
7. provide appropriate filtering and monitoring systems;
8. ensure that online safety incidents are identified, reported, investigated and responded to appropriately;
9. support pupils and families in understanding online risks;
10. protect school systems, devices, accounts and information from misuse, unauthorised access and cyber threats;
11. promote respectful and professional online communication;
12. ensure that emerging technologies, including generative AI, are used safely and responsibly;
13. protect personal and confidential information; and
14. regularly review the effectiveness of the school's online safety arrangements.

This policy applies to all members of The Online School UK community, including:

- pupils
- teachers
- Happiness Manager Leads
- Happiness Manager Assistants
- the Senior Leadership Team
- the Designated Safeguarding Lead (DSL) and Deputy DSLs

- administrative staff
- volunteers
- contractors
- visitors
- parents/carers where they interact with school systems or members of the school community
- any other person authorised to use the school's ICT facilities or platforms i.e. teachers or students

It applies to the use of:

- school-owned or school-managed devices
- personal devices when used for school purpose
- school networks and system
- school email accounts
- online learning platforms
- live lesson platforms
- school communication platforms
- messaging systems
- cloud storage
- school social media accounts
- websites and web applications
- artificial intelligence and generative AI tools
- telephony systems
- digital records and files
- any other technology or digital service used for school purposes

The policy applies whether technology is being accessed from school, from home or from another location.

3. Roles and Responsibilities

Director

The Director strategic responsibility for ensuring that appropriate arrangements are in place to safeguard pupils online.

This includes ensuring that:

- online safety is incorporated into the school's safeguarding arrangements;
- appropriate filtering and monitoring systems are in place;
- the effectiveness of filtering and monitoring is reviewed at least annually;
- appropriate resources are available;
- staff receive appropriate training;

- online safety risks are appropriately assessed;
- policies are reviewed and updated;
- significant online safety concerns are appropriately addressed; and
- leaders are held accountable for the effectiveness of online safety arrangements.

SLT Team- CEO and Headteacher

The Headteacher is responsible for:

- implementing this policy
- ensuring that staff understand their responsibilities
- ensuring that online safety forms part of the school's safeguarding culture
- overseeing responses to serious online safety incidents
- supporting the DSL and relevant staff
- ensuring that appropriate disciplinary or behavioural procedures are followed where required
- ensuring that this policy is reviewed

Further Senior Leadership Team, including the Business Manager and the DSL, will:

- support the implementation of this policy
- ensure that online safety concerns are dealt with appropriately
- monitor compliance with the policy
- ensure appropriate staff training
- manage staff-related concerns in accordance with relevant procedures
- ensure that online safety is reflected in wider school policies
- support the DSL and Developer/IT support
- ensure that lessons are learned from online safety incidents

Designated Safeguarding Lead

The DSL has lead responsibility for online safeguarding within the school's wider safeguarding arrangements.

The DSL will:

- understand the school's online safety risks
- work with the Developer/IT support to understand filtering and monitoring arrangements
- ensure that online safety concerns are appropriately considered as safeguarding concerns
- ensure that staff know how to report online safety concerns
- ensure that concerns involving pupils are assessed and responded to appropriately
- liaise with parents/carers and external agencies where appropriate

- ensure that safeguarding information arising from online incidents is recorded appropriately
- contribute to staff training
- contribute to the annual review of filtering and monitoring
- ensure that online safety is reflected in safeguarding and child protection arrangements
- review emerging online risks and consider whether the school's practice needs to change
- managing all online safety issues and incidents in line with the school safeguarding policy
- ensuring that any incidents of online-bullying are logged and dealt with appropriately in line with the school behaviour and anti-bullying policies

Developer / IT Support

The school's Developer/IT support is responsible for the technical management of ICT systems and works with the DSL, Senior Leadership Team and relevant staff to support online safety.

This includes:

- maintaining appropriate system security;
- managing access permissions;
- maintaining filtering and monitoring arrangements;
- responding to technical security incidents;
- supporting the investigation of online safety incidents where appropriate;
- maintaining appropriate system access controls;
- supporting cyber security arrangements;
- reporting significant technical or safeguarding concerns to the appropriate senior staff; and
- supporting the annual review of filtering and monitoring.

Technical staff with access to monitoring information will receive appropriate safeguarding and online safety training.

Staff (Teaching and Non Teaching)

All staff are responsible for:

- safeguarding pupils online
- modelling safe and professional online behaviour
- following this policy and the school's Acceptable Use requirements
- reporting online safety concerns promptly
- following safeguarding procedures where online activity raises a concern about a pupil
- maintaining appropriate professional boundaries

- protecting school and pupil information
- using school systems appropriately
- completing required online safety and safeguarding training
- remaining alert to emerging online risks
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to acceptable use of the school's teacher dashboard, Big Blue Button platform and Slack
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Staff must not assume that an online incident is merely a behaviour or technical issue where there may be a safeguarding element.

Students

Pupils are expected to:

- use school technology responsibly
- follow the school's Acceptable Use requirements
- follow the school's Behaviour Policy, including out of school conduct, in line with online safety
- treat others respectfully online
- report harmful, inappropriate or concerning online behaviour
- protect their passwords and accounts
- not attempt to bypass filtering or monitoring
- not access or share inappropriate material
- not share personal information unnecessarily
- use AI responsibly and in accordance with school expectations
- follow staff instructions concerning online safety

Parents and Carers

Parents and carers play an important role in supporting children to stay safe online.

The school will:

- provide information and guidance about online safety where appropriate
- communicate relevant concerns where appropriate
- encourage parents/carers to discuss online safety with their children
- signpost families towards reliable online safety resources
- encourage families to use appropriate parental controls and filtering where possible

Because pupils access lessons from home, the school recognises that it cannot control every aspect of a pupil's home internet environment. Parents/carers are therefore encouraged to take appropriate steps to support safe internet use at home.

4. Education and Curriculum

Online safety education will be embedded within the school's curriculum via Life Skills and PSCE, and will form a part of our schools wider safeguarding approach.

The curriculum will be age-appropriate, developmentally appropriate and responsive to emerging online risks. It will support students to understand:

- how to use technology safely and responsibly, including the appropriate use of social media and artificial intelligence;
- how to recognise online risks, including harmful or inappropriate content, and the impact of viewing harmful content;
- how to respond to unwanted contact and identify harmful behaviours online, including bullying, abuse, harassment, grooming and exploitation;
- how to maintain healthy digital relationships, communicate respectfully and recognise consent from others, including sexual consent, and how and when consent can be withdrawn in all contexts, including online;
- how to report concerns, report harmful material and where to get support if they have been affected by harmful online behaviours;
- how to protect personal information and understand how information and data is generated, collected, shared and used online;
- the risks associated with sharing personal, private or compromising material online, including that material provided to another person has the potential to be shared further and may be difficult to remove;
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- the risks associated with sharing and viewing nude, semi-nude or indecent images, including that sharing and viewing indecent images of children, including those created by children, is a criminal offence which carries severe penalties;
- online sexual harassment, harmful sexual behaviour and the impact that sexually explicit material, including pornography, can have on attitudes, relationships and behaviour;
- misinformation and disinformation, online scams, fraud and financial exploitation;

- extremist and harmful content, including how to build resilience to radicalisation and how online content can influence individuals;
- digital footprints and online reputation, including the potential long-term impact of online activity;
- copyright and intellectual property;
- how online activity can affect wellbeing and mental health;
- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online; and
- how to participate positively and safely online, including providing a safe environment for debating controversial issues and understanding how they can influence and participate in decision-making.

Online safety education will be age-appropriate and responsive to the needs and risks of individual pupils.

The school will consider whether pupils with SEND or other additional needs require adapted or additional online safety education. ***This may include further educational support and resources provided to homes to do at home education.***

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND and mental health needs.

5. Online Learning and Live Lessons including cameras, microphones and lesson conduct

The Online School UK uses our own developed online platform (the Dashboard) as well as Big Blue Button for live lessons. Senior Leadership and the Happiness Manager team will continue to monitor dashboard and live lesson usage each day, including the use of our in-house Message Board. Only current enrolled students, teachers and staff members have access to live lessons and their recordings.

The Online School UK uses Big Blue Button for delivering live and recorded lessons. Only authenticated users will be permitted to enter live classes:

- Teachers and admin have the ability to remove any user from the live lesson, and prevent them from returning, if there are any safeguarding concerns of a particular user
- Teachers are always visible on webcam as per the teacher standards and expectations policy
- All lessons are recorded for safeguarding purposes, lesson observations and for later review by students

- Use of cameras and microphones are encouraged to build community in our classrooms, however these are not pressured or expected. Students have multiple options for communication in classrooms, including the public chat (visible to all users), polls (anonymous and only seen by teachers and admins), private messages to teachers and admins and the microphone. All of these can also be utilised with or without a student's camera on. Classrooms are automatically set to only teachers and admins being able to view cameras in live lessons, but this can be changed with student consent.
- Teachers have the ability to turn off the webcams and microphones of students, one at a time or in bulk
- Teachers have the ability to control who is sharing their screen and annotating documents/images
- students are able to communicate with the teacher publicly using the chat function in Big Blue Button or privately via private message in lesson, or the Message Board outside of lesson
- Only authenticated users are permitted to access lesson recordings, posted on the Student Dashboard's 'Lessons' page
- Only key administrators will be given access to Big Blue Button's admin control functions
- The unique login and password details for accessing school sites should be kept securely, to prevent unauthorised access

As an online school, we take particular care to ensure that live lessons and online learning are safe and appropriate.

Staff must:

- use only approved school platforms for lessons and curriculum management
- follow the Staff Communication and Conduct Policy
- maintain appropriate professional boundaries
- use appropriate backgrounds and environments
- don't share personal contact details
- use school-approved communication systems
- ensure that lesson content is appropriate
- report safeguarding concerns
- manage chat functions appropriately
- avoid unnecessary one-to-one communication with pupils outside approved systems
- follow the school's procedures for recording or retaining online lessons

By enrolling with The Online School UK, parents and carers consent to their child or young person participating in video conferencing via Big Blue Button, including the use of chat, webcam and microphone functions.

Live Lessons

The Online School will ensure that lesson recordings are only available to students enrolled in that particular class, their teachers, Happiness Managers (admin team) and the Headteacher. All Live Lessons are recorded and held in a secure location in case it needs to be reviewed for academic or safeguarding purposes.

- Computers and laptops should be in an appropriate location
- Language will be appropriate and professional, including any family members/friends in the background
- When you are not talking, ensure that your microphone is muted
- Avoid talking over other students where possible. If you want to contribute to the discussion, then use the 'raise hand' function and wait for the teacher to call upon you or a natural break in the conversation
- Behaviour on camera needs to be sensible and appropriate at all times

There may be a specific reason why students feel they cannot appear on webcam during lessons. This is understandable and we are happy for students to remain off camera in lessons, however we encourage parents/carers to share any concerns about this to their child's Happiness Manager Lead.

There are 3 categories of lesson contribution that students can make:

1. Contribute by public chat, answering private poll questions, sending private messages to teachers and/or Happiness Managers, collaborating by writing on whiteboards, and by sharing my work
2. Contribute by public chat, answering private poll questions, sending private messages to teachers and/or Happiness Managers, collaborating by writing on whiteboards, by sharing my work and on mic
3. Contribute by public chat, answering private poll questions, sending private messages to teachers and/or Happiness Managers, collaborating by writing on whiteboards, by sharing my work, on mic, and on camera

Camera Expectations

Our expectation is that all teachers will use webcam when delivering lessons online, and we also facilitate students using webcams during lessons, though this is at their discretion. We have found that there are many benefits for students using webcams during lessons:

- Building a sense of community amongst students
- Teachers can interpret visual cues, e.g. recognising when a student is 'stuck' and needs help
- students can quickly show the work they have completed, and teachers can give feedback or address misconceptions during the live lesson, rather than waiting to see an uploaded assignment.

To keep all of our students and staff safe, all teachers and students using webcams during lessons are required to adhere to our user guidelines.

- Users should be dressed appropriately at all times.
- Users should behave appropriately at all times.

- Users should consider the webcam background, e.g. wall displays and items behind them that will be visible to others.
- Other people should not be visible on webcam during lessons, e.g. parents or sibling, unless their presence is purely to support the student in their learning.

Should the above guidelines not be followed, our Safeguarding team will investigate and respond accordingly. These next steps may include:

- A removal of camera permissions
- Communication home with parents to discuss concerns
- Escalation to outside agencies dependent on the consistency and/or the severity of the behaviour displayed on camera

More details of potential next steps can be seen on the Use of Mic, Cam, and Public Chat Features section of our website.

6. Communication and Professional Boundaries

The Online School UK requires staff to maintain clear professional boundaries when communicating online.

Staff must use school-approved systems for work-related communication.

Administrative staff, including the Senior Leadership Team, Happiness Managers and Happiness Manager Assistants, will use school-provided email accounts for work-related communication where required.

Other staff should use Slack for work communication, except in emergency circumstances where WhatsApp may be used to contact a staff member, and the internal Message Board for student/parent communication outside live lessons, in accordance with school procedures.

Staff must not:

- share personal email addresses with pupils or parents/carers
- send work-related materials using personal email accounts
- share personal telephone numbers with pupils or parents/carers
- communicate with pupils through personal social media accounts
- use personal messaging accounts for routine school business
- communicate with pupils in a way that undermines professional boundaries
- use staff and school platforms for personal use i.e. curriculum sites for other materials

Where staff need to make telephone calls to parents/carers, the school-approved CircleLoop system should be used.

Where a personal device must be used in exceptional circumstances, the member of staff should follow the school's procedures, protect their personal information and ensure appropriate professional boundaries are maintained.

Staff Email

Staff must use school-provided email accounts for work purposes where such accounts are provided.

Staff must:

- take care when composing and sending emails
- protect confidential information
- check recipients before sending sensitive information
- use encryption where appropriate
- report emails received in error
- report data breaches immediately
- avoid unnecessary sharing of personal information
- use professional language
- retain or delete information in accordance with school procedures

Staff should be aware that electronic communications may be retained and may be subject to lawful disclosure.

If staff send an email containing another person's personal information to an incorrect recipient, they must immediately inform the Headteacher, Business Manager or DSL and follow the school's data breach procedure.

Staff Phones and Personal Devices

Staff must use personal devices responsibly where they are used for school purposes.

Staff must:

- maintain professional boundaries
- protect school information
- use appropriate security measures
- not store school or pupil data unnecessarily on personal devices
- not allow other people to access confidential school information
- follow school procedures concerning photographs, recordings and communications
- report lost or compromised devices where school information may be affected

School or pupil information temporarily downloaded to personal or unmanaged hardware for an immediate operational purpose must be permanently deleted when the task is complete, unless otherwise authorised.

Long-term storage or syncing of The Online School UK data on personal devices is not permitted unless expressly authorised.

Staff Personal Use of Social Media

- All students use their own personal email address within the school systems
- students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the DSL / Headteacher / Happiness Manager Lead / Happiness Manager Assistant, or another member of staff.
- Safe and appropriate use of social media will be taught to students as part of online safety education, via age-appropriate sites and resources
- Any concerns regarding students' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Staff Personal Use

Staff may occasionally use school ICT facilities for reasonable personal purposes, provided that such use:

- does not take place during teaching or other working time where it interferes with duties;
- does not constitute unacceptable use;
- does not take place in the presence of pupils where inappropriate;
- does not interfere with the work of the school;
- does not compromise school systems or data; and
- does not breach any other school policy.

Staff must not use school ICT facilities to store personal, non-work-related information or materials, except where specifically permitted by the school, such as the Staff Social channel on Slack for appropriate staff socialisation.

Staff should be aware that use of school ICT facilities may be subject to lawful filtering and monitoring.

Personal use of social media and other online platforms outside school systems may still have employment implications where it affects professional conduct, safeguarding, confidentiality or the reputation of the school.

Staff Access to Platforms and Materials

The school's Developer manages access to ICT facilities, while the Senior Leadership Team manages access to relevant staff materials.

This may include:

- access permissions for school platforms
- access permissions for programmes
- access to school files
- access to communication systems
- other role-specific permissions

Access will be provided according to role and need.

Staff must only access information that they are authorised to access.

If a member of staff has access to information they are not authorised to view or edit, they must inform the Headteacher or Business Manager.

Senior Leadership Team and authorised administrative staff will be provided with appropriate unique account information and passwords.

The Senior Leadership Team and Developer may have appropriate administrative access to staff accounts for legitimate safeguarding, security, technical and operational purposes.

Access may be removed immediately where necessary, including when a staff member leaves the school or where safeguarding or security concerns require this.

All staff must follow the school's cyber security protocols.

7. Acceptable Use

Information and communications technology (ICT) is an integral part of the way our school works and is a critical resource for all members of The Online School UK community. As an online school, it is fundamental to our teaching and learning, safeguarding, pastoral and administrative functions of the school.

Maintaining system and device security is the responsibility of the school's Developer. Any concerns should be reported to our Business Manager, who will relay this communication to the Senior Leadership Team, DSL and Developer to ensure online safety and security measures are met.

However, the ICT resources and platforms our school uses could also pose risks to data protection, online safety and safeguarding.

This section of the policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers

- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This section covers all users of our school's ICT facilities, including staff, pupils, parents, volunteers, contractors and visitors.

All users are expected to use the school's ICT facilities responsibly, legally, safely and respectfully.

Acceptable use includes:

- accessing systems for legitimate educational, professional or administrative purposes
- communicating respectfully
- protecting passwords and accounts
- respecting copyright and intellectual property
- protecting personal and confidential information
- reporting concerns
- following school policies
- using approved software and services
- using AI only where permitted
- following staff instructions
- using school systems in a way that supports learning, safeguarding and the effective operation of the school

Acceptable Use of the Internet and School Systems

All students, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's IT systems.

Use of the school's systems such as Dashboards and Big Blue Button must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

How Will the School Respond to Misuse of IT Systems?

Where a pupil misuses the school's online systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. 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 online systems 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.

Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities/platforms. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on the school's platforms without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the platforms, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities/platforms
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):

- o During assessments, including internal and external assessments, and coursework
- o To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

The school may update the list as technology and online risks develop.

Breaches of this section of the policy may be dealt with under our Disciplinary Policy, Behaviour Policy, Staff Discipline Policy and/ or Staff Communication and Conduct Policy

8. Artificial Intelligence and Generative AI

The Online School UK recognises that artificial intelligence can provide educational and administrative benefits but also presents safeguarding, data protection, intellectual property, accuracy and ethical risks.

Any use of AI must be safe, appropriate and proportionate.

The school will consider:

- age restrictions
- safeguarding
- filtering and monitoring
- data protection
- privacy
- intellectual property
- misinformation and inaccurate information
- bias and discrimination
- inappropriate or harmful content
- manipulation
- mental health and wellbeing
- academic integrity
- the impact on teaching and learning

The school will only approve AI tools where appropriate safeguards have been considered.

Pupils may use AI tools:

- as a research tool to explore new topics and ideas;
- where specifically directed as part of teaching and learning;
- when studying AI and its applications; and
- for other purposes expressly authorised by the school or teacher.

All AI-generated content must be appropriately acknowledged or attributed where required.

Pupils must not use AI:

- during assessments where its use is not permitted;
- to complete homework or assignments where AI use is not authorised;
- to present AI-generated work as entirely their own where this would breach academic expectations;
- to create harmful, abusive or sexual content;
- to create or manipulate images of pupils or other people in a harmful manner;
- to impersonate another person;
- to generate content designed to deceive or defraud; or
- to circumvent school safeguarding or monitoring arrangements.

Staff must not enter pupil personal data, special category data, confidential school information or other sensitive information into publicly available AI tools unless the tool has been approved and appropriate data protection requirements have been met.

Staff remain responsible for checking the accuracy, appropriateness and suitability of AI-generated content.

The DfE's current guidance emphasises that AI use by staff and pupils must be carefully considered, risk-assessed and aligned with safeguarding, data protection and other legal obligations.

9. Cyber Security

All users have a responsibility to protect the school's ICT systems and information.

Users must:

- keep passwords confidential;
- use strong passwords;
- not share accounts;
- use multi-factor authentication where required;
- lock or secure devices when not in use;
- report suspicious activity;
- report suspected phishing;
- not install unauthorised software;
- not disable security controls;
- not connect unauthorised devices where prohibited;
- follow cyber security instructions;
- keep software and devices appropriately updated; and
- report lost or stolen devices immediately.

Users must not attempt to test, defeat or circumvent the security of the school's systems unless specifically authorised to do so.

The school will maintain appropriate technical and organisational measures to reduce cyber security risks.

10. Social Media

The Online School UK recognises that social media forms part of the wider online environment in which pupils, staff and families may communicate and interact.

The school acknowledges that activity taking place outside the school's platforms may affect pupils, staff or the wider school community. Where online activity raises safeguarding, bullying, harassment, discriminatory behaviour or professional conduct concerns, the school may need to respond in accordance with its safeguarding, behaviour or staff conduct procedures.

Pupils

Pupils are expected to use social media responsibly and in accordance with the school's expectations for respectful and safe online behaviour.

Pupils must not:

- use social media to bully, harass, threaten or intimidate another person;
- share another person's personal information without permission;
- share images, recordings or other content involving another pupil or member of staff without appropriate permission;
- create or share content intended to humiliate, threaten or cause harm to another person;
- impersonate members of staff or other pupils;
- use social media to distribute discriminatory, abusive, hateful or otherwise harmful content;
- use social media to share confidential school information; or
- use social media to arrange inappropriate or unsafe contact with other pupils.

Where social media activity affects the welfare or safety of a pupil or member of the school community, the school will consider the matter in accordance with its safeguarding and other relevant procedures.

Staff

Staff are expected to maintain appropriate professional boundaries when using social media.

Staff must not use personal social media accounts to establish inappropriate or unauthorised relationships with pupils or to communicate with pupils outside approved school communication systems.

Staff must:

- maintain professional boundaries with pupils and families;
- avoid sharing confidential or personal school information through personal social media accounts;
- avoid posting content that could reasonably undermine professional relationships, safeguarding or confidence in the school;
- follow the Staff Code of Conduct and relevant staff policies; and
- report any safeguarding concern arising through social media in accordance with the school's safeguarding procedures.

Staff should be aware that online content may remain accessible or be shared beyond its original intended audience and should exercise appropriate professional judgement.

Where concerns arise regarding staff use of social media, these will be considered in accordance with the school's Staff Communication and Conduct Policy, Staff Disciplinary Policy, Safeguarding and Safeguarding and Child Protection Policy.

11. Online Bullying, Harassment and Harmful Behaviour

The Online School UK does not tolerate cyberbullying, harassment, discriminatory behaviour or other harmful online conduct.

This includes behaviour through:

- online lessons
- message boards
- messaging applications
- social media
- gaming platforms
- email
- private messaging
- group chats
- other digital environments

Where online behaviour involves pupils, it may constitute a safeguarding concern even where the behaviour takes place outside school or outside school-managed systems.

Staff must report concerns to the DSL or Deputy DSL in accordance with safeguarding procedures.

The school will consider the circumstances, risks and impact of the behaviour and will take appropriate action.

Cyber-Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Happiness Manager Leads and Life Skills teachers will discuss cyber-bullying with the students as well as it being addressed with assemblies.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful behaviour or material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal.

The DSL will also work with differing external services if it is deemed necessary to do so such as Children's Social Care and Children's Exploitation and Online Protection agency, CEOP.

In an event where an incident of cyberbullying is identified, no matter which external service or pathway are contacted, parents of those involved will be supported as necessary. This may include but is not limited to: providing Online Safety Resource Booklets, advice on how to report to CEOP, NSPCC guidance and more.

Sexual Harassment, Sexual Violence and Sharing of Nude or Semi-Nude Images

The school recognises that technology can facilitate sexual harassment, sexual violence and the sharing of nude or semi-nude images.

Staff must take concerns seriously and must not dismiss behaviour as "banter", joking or normal online behaviour where it causes or has the potential to cause harm.

Where a pupil is involved in the creation, sending, requesting, receiving or distribution of nude or semi-nude images, staff must follow safeguarding procedures and report the concern to the DSL.

Staff must not:

- forward or copy such images
- save them unnecessarily
- investigate independently beyond their safeguarding role
- share them with colleagues except where required through appropriate safeguarding procedures

The DSL will manage concerns in accordance with the Safeguarding and Child Protection Policy and relevant national guidance.

Online Grooming, Exploitation and Abuse

The school recognises that children may be groomed or exploited through online platforms.

Staff should remain alert to:

- changes in behaviour
- secretive online activity
- unexplained contact with adults or unknown individuals
- inappropriate sexualised behaviour
- unexplained gifts or money
- involvement in harmful online communities
- threats or coercion
- requests for images
- blackmail
- suspicious accounts or contacts
- other indicators of exploitation or abuse

Any concern must be reported to the DSL in accordance with safeguarding procedures.

Extremism, Radicalisation and Harmful Online Content

The school recognises that pupils may encounter extremist or radicalising content online.

This may include:

- extremist propaganda
- terrorist material
- hate speech
- misogynistic or violent extremist material
- content encouraging violence
- conspiracy theories
- recruitment material
- online communities that seek to manipulate or radicalise children

Staff must report concerns through safeguarding procedures.

The DSL and Prevent Lead will consider Prevent responsibilities where appropriate.

The school will also support pupils to develop critical thinking and resilience when encountering misleading, manipulative or harmful online content.

12. Filtering and Monitoring

The Online School UK uses a combination of **platform safeguards, automated filtering, staff supervision, monitoring and safeguarding procedures** to help protect pupils from online harm.

As an online school, filtering and monitoring are an important part of our safeguarding arrangements and are used to help reduce pupils' exposure to harmful or inappropriate content and to identify potential safeguarding concerns.

The school recognises that filtering and monitoring systems cannot identify every harmful, inappropriate or AI-generated piece of content and that technical limitations may exist. Filtering and monitoring therefore form **part of, rather than replace, the school's wider safeguarding arrangements**.

The school's filtering and monitoring arrangements apply to relevant school-managed platforms and systems used by pupils, including the school's online learning environment.

Filtering

The school uses automated filtering and platform safeguards to reduce pupils' exposure to inappropriate, offensive or harmful material.

Our platform includes safeguards designed to:

- filter inappropriate or offensive language within public lesson chat;
- automatically block racist, discriminatory, abusive or otherwise inappropriate language before it is visible to other pupils;
- prevent pupils from sharing personal contact information in public chat, including email addresses, telephone numbers and social media usernames or links;
- apply similar filtering to the school's message boards to help prevent the sharing of personal contact details or inappropriate content; and
- restrict pupils from accessing or sharing content that is identified by the school's filtering arrangements as inappropriate or harmful.

The school will also consider the risks associated with pupils using **generative artificial intelligence and other AI-enabled platforms**.

Where pupils are permitted to use AI tools, the school will seek to ensure that appropriate safeguards are in place to reduce the risk of pupils accessing or generating harmful or inappropriate content.

The school recognises that AI-generated content may present particular challenges for filtering systems. The fact that content has been generated by an AI system does not remove the need for the school to consider whether that content is harmful or inappropriate.

Filtering arrangements will therefore be considered alongside monitoring, staff supervision, online safety education and wider safeguarding procedures.

Monitoring

The school uses monitoring arrangements to help identify potential online safety, safeguarding and wellbeing concerns.

Depending on the platform or system being used, monitoring may include:

- public lesson chat
- student message boards
- lesson recordings
- safeguarding incidents
- behaviour concerns
- other relevant activity within school-managed online systems.

All live lessons are actively supervised by the class teacher and, where appropriate, a Happiness Manager or Teaching Assistant.

During live lessons, staff will:

- monitor pupil participation and behaviour;
- supervise public chat;
- respond to safeguarding or wellbeing concerns;
- support pupils through private staff-to-pupil messaging where appropriate; and
- intervene promptly where behaviour does not meet the school's expectations.

Pupils are unable to send private messages to one another through the school's platform. Private messaging is restricted to communication between pupils and authorised members of staff, such as teachers and Teaching Assistants/Happiness Managers.

Monitoring arrangements are intended to help the school identify concerns quickly and support appropriate intervention.

Responding to Filtering and Monitoring Concerns

Where filtering or monitoring identifies potentially harmful, inappropriate or concerning activity, the concern will be considered in accordance with the school's safeguarding procedures.

Any concern which may indicate that a pupil is at risk of harm must be reported to the **Designated Safeguarding Lead (DSL)** or Deputy DSL in accordance with the Safeguarding and Child Protection Policy.

The DSL will determine what further action is required.

Where a concern is primarily technical, it may also be referred to the appropriate IT support.

Staff must not treat a safeguarding concern identified through filtering or monitoring as solely a technical issue.

Where appropriate, concerns and actions will be recorded to support safeguarding, monitoring, review and learning.

Limitations of Filtering and Monitoring

The school recognises that:

- filtering systems may not identify every form of harmful content
- monitoring systems may not identify every concerning interaction or behaviour
- AI-generated content may present particular filtering challenges
- technical failures or limitations may occur
- pupils may use devices, networks or platforms outside the school's control
- online risks can change rapidly

Filtering and monitoring must therefore be used alongside:

- effective safeguarding procedures;
- staff supervision;
- online safety education;
- appropriate staff training;
- professional judgement;
- communication with parents/carers where appropriate; and
- other technical and organisational safeguards.

The absence of an alert or filtering block must not be interpreted as evidence that a pupil is safe.

Staff remain responsible for reporting safeguarding concerns even where those concerns have not been identified through the school's filtering or monitoring systems.

Filtering and Monitoring Review

The effectiveness of the school's filtering and monitoring arrangements will be reviewed at least once every academic year.

The review will be led by the member of the Senior Leadership Team responsible for filtering and monitoring, with support from the Designated Safeguarding Lead (DSL) and appropriate IT support.

The school will maintain records of the review, checks undertaken and any actions arising.

The review will consider whether filtering and monitoring arrangements remain appropriate for the school's online learning environment and pupil risk profile.

Annual Review

The annual review will include checks that filtering and monitoring arrangements are functioning appropriately across relevant school-managed internet-connected systems and locations.

The review will consider:

- whether filtering is working as intended
- whether monitoring is identifying relevant risks
- whether users can be appropriately identified
- whether safeguarding alerts are reaching the appropriate staff
- the use and risks associated with generative AI
- technical limitations of the school's systems
- online safeguarding incidents and trends
- pupil risk profiles
- whether staff understand the reporting process
- whether the school's online learning environment has changed in a way that affects filtering or monitoring
- whether the school's current arrangements remain proportionate and appropriate; and
- whether any changes or improvements are required

The school will also consider whether filtering and monitoring arrangements continue to support the school's curriculum and legitimate educational use without unnecessarily restricting appropriate access to learning resources.

Review Following Incidents or Changes

Filtering and monitoring arrangements may also be reviewed outside the annual cycle where:

- a significant safeguarding incident occurs;
- a significant filtering or monitoring failure is identified;
- new technology or platforms are introduced;
- significant changes are made to the school's online learning environment;
- new online risks emerge;
- there is evidence that existing filtering is not working as intended; or
- there is reason to believe that monitoring is no longer appropriately identifying relevant risks.

Where a significant safeguarding concern is identified through filtering or monitoring, this will be reported to the DSL **without delay** and dealt with in accordance with the school's safeguarding procedures.

Records and Actions

A record of the filtering and monitoring review will be maintained.

This will include, where appropriate:

- checks undertaken
- findings
- identified limitations
- safeguarding or technical concerns
- actions required
- person responsible for each action
- confirmation of actions completed

Actions identified through the review will be followed up to ensure that identified weaknesses or risks are appropriately addressed.

The school will use information from filtering and monitoring incidents and annual reviews to identify trends, inform safeguarding practice, support staff training and determine whether changes to the school's online safety arrangements are required.

13. Data Protection and Privacy

All users must protect personal information belonging to pupils, parents/carers, staff and other members of the school community.

Users must:

- only access personal information where authorised;
- only share information where there is a legitimate reason;
- use secure communication systems;
- avoid unnecessary downloading of personal information;
- protect passwords;
- report suspected data breaches immediately;
- follow the school's Data Protection Policy; and
- follow the school's privacy notices.

Filtering and monitoring information will only be accessible to authorised personnel.

Where third-party filtering, monitoring or AI systems process personal data, the school will consider data protection requirements, including appropriate contracts, privacy information and Data Protection Impact Assessments where required.

Current DfE guidance specifically states that schools should consider what monitoring data is collected, who can access it and how long it is retained, and should conduct a DPIA before introducing a new filtering or monitoring system or making significant changes.

14. Online Safety Incidents and Reporting

The Online School UK recognises that online safety incidents may arise through teaching and learning platforms, school-managed devices and accounts, communication systems, social media, gaming platforms, personal devices used to access school activities, or other online environments.

Online safety incidents will be treated as part of the school's wider safeguarding, child protection, health and safety, behaviour and information-security arrangements.

All members of the school community are expected to report online safety concerns promptly. Staff and pupils should not attempt to investigate or resolve safeguarding concerns themselves where doing so could place a pupil or another person at further risk.

Online safety concerns may include, but are not limited to:

- exposure to illegal, inappropriate or harmful content
- online bullying or harassment
- sexual harassment or harmful sexual behaviour online
- grooming, exploitation or inappropriate contact from an adult or another user
- the sharing or attempted sharing of intimate images
- threats, coercion, blackmail or intimidation
- extremist or terrorist content or concerns relating to radicalisation
- misogynistic, discriminatory or hateful content

- harmful online challenges or activities
- identity theft, impersonation or compromised accounts
- phishing, scams or other cyber-enabled abuse
- unauthorised access to school systems
- inappropriate use of artificial intelligence or AI-generated harmful content
- unauthorised recording, photography, screenshots or distribution of online lessons
- inappropriate use of school platforms, systems or accounts
- disclosure or loss of personal or confidential information
- suspected data breaches
- inappropriate contact or communications involving staff and pupils
- unauthorised participants entering online lessons or meetings
- any other online activity that may place a pupil, member of staff or other person at risk of harm.

Reporting Safeguarding Concerns

Where an online incident or concern may relate to the safety or welfare of a child, it must be reported to the Designated Safeguarding Lead (DSL) or Deputy DSL without delay, in accordance with the school's Child Protection and Safeguarding Policy.

Staff must act immediately where there is a concern that a child may be at risk of harm. Concerns must not be delayed because the incident occurred outside normal school hours, outside the school's online platform, or outside the physical school environment.

Where a child is in immediate danger, the appropriate emergency services should be contacted in accordance with the school's safeguarding procedures.

The school will maintain appropriate records of safeguarding and significant online safety concerns. Records should include, where relevant:

- the nature of the concern or incident;
- the date and time;
- the individuals involved;
- information or evidence available;
- actions taken;
- decisions made;
- the rationale for decisions;
- referrals or escalations made; and
- outcomes and follow-up actions.

Information will be shared on a need-to-know basis and in accordance with safeguarding and data protection requirements. Data protection requirements must not be used as a reason to prevent necessary information sharing where this is required to protect a child.

Evidence and Digital Content

Where an online safety incident may require investigation, safeguarding action or reporting to an external agency, relevant evidence should be preserved where appropriate and lawful.

Staff and pupils should not forward, copy, download or redistribute harmful or illegal material unnecessarily.

Where an incident involves potentially illegal or harmful sexual imagery involving a child, staff must follow the school's safeguarding procedures and must not intentionally view, copy, save or distribute material beyond what is necessary to follow those procedures.

Concerns About Staff

Any concern about the online conduct of a member of staff, volunteer, contractor or other adult working with pupils must be reported and managed in accordance with the school's procedures for allegations against staff and low-level concerns. These can be found on our Whistleblowing Policy and Complaints Policy.

This includes concerns arising from:

- inappropriate online communication with pupils
- inappropriate use of personal accounts or messaging services
- inappropriate online behaviour
- inappropriate sharing or viewing of material
- breaches of professional boundaries
- other behaviour that may indicate a risk to pupils

The school will ensure that online safeguarding concerns involving staff are escalated to the appropriate person and managed in accordance with KCSIE and the school's safeguarding procedures.

15. Staff Training

The Online School UK will ensure that staff receive appropriate training to enable them to understand, identify, prevent and respond to online safety risks.

Online safety will form part of the school's wider safeguarding training and will not be treated as a separate technical issue.

All staff will receive appropriate information and training on:

- the school's online safety and acceptable-use requirements;
- the school's safeguarding and child protection procedures;

- the role and responsibilities of the DSL and Deputy DSL;
- recognising online abuse, exploitation and other online harms;
- the four areas of online risk: content, contact, conduct and commerce;
- cyberbullying, harassment and harmful online behaviour;
- online sexual abuse, grooming and exploitation;
- harmful sexual behaviour and the sharing of intimate images;
- extremist and terrorist content and online radicalisation;
- appropriate professional boundaries when working online;
- safe use of school platforms and communication systems;
- appropriate use of school-managed devices and accounts;
- filtering and monitoring arrangements;
- reporting and escalation procedures;
- data protection and information security;
- phishing, scams, compromised accounts and other cyber risks;
- the responsible use of artificial intelligence and emerging technologies; and
- how and where to obtain further advice and support.

Training will be appropriate to the role and responsibilities of the individual.

Staff with specific responsibilities for safeguarding, filtering and monitoring, information security, technical administration or online safety will receive additional role-specific training where required.

The DSL will ensure that staff understand how online safety concerns identified through teaching, communications, filtering, monitoring or other school systems should be escalated.

Staff will receive appropriate updates when significant changes occur to:

- online risks;
- legislation or statutory guidance;
- school procedures;
- technology or platforms used by the school; or
- the school's filtering, monitoring or security arrangements.

The effectiveness of online safety training will be reviewed through safeguarding reviews, incident analysis, staff feedback, audits and other appropriate evaluation.

Staff are expected to maintain an appropriate level of awareness of emerging online risks and to seek advice where they are uncertain about how to respond to an online safety concerns.

16. Supporting Parents and Carers

The Online School UK recognises that parents and carers play an important role in supporting children to remain safe online, particularly where pupils access education from home or other locations outside the school's direct physical supervision.

The school will provide parents and carers with appropriate information and guidance to support safe and responsible use of technology.

This may include information about:

- the online platforms and services used by the school;
- how pupils access online lessons and learning resources;
- appropriate online behaviour;
- safeguarding risks associated with online activity;
- the school's filtering and monitoring arrangements;
- how online safety concerns can be reported;
- how parents and carers can raise concerns about a pupil's online experience;
- parental controls and other safety tools;
- privacy and account security;
- online bullying and harmful behaviour;
- online sexual exploitation and grooming;
- harmful online content;
- age restrictions and appropriate use of online services;
- artificial intelligence and emerging online risks; and
- sources of further advice and support.

The school will make clear to parents and carers:

- what pupils are expected to do online;
- which websites, applications and platforms pupils may be required to access;
- who pupils may interact with online as part of their education;
- how pupils can report concerns;
- how the school can be contacted about online safety matters; and
- the limits of the school's ability to monitor activity occurring outside school-managed systems.

Parents and carers will be encouraged to discuss online safety with their children and to establish appropriate expectations and boundaries for technology use at home.

The school will signpost parents and carers to appropriate sources of online safety information and support.

Where an online safety concern relates to the safeguarding or welfare of a pupil, the school will work with parents and carers where appropriate and in accordance with the school's safeguarding procedures.

The school will recognise that parental involvement may not always be appropriate or safe in individual safeguarding circumstances. Decisions about information sharing with parents and carers will therefore be made in accordance with the school's safeguarding procedures and the best interests of the child.

17. Accessibility/ Vulnerable Students

The school recognises that online risks may affect pupils differently and that some pupils may require additional support to access online learning safely.

The school will consider the individual needs, age, developmental stage, circumstances and vulnerabilities of pupils when developing and implementing online safety arrangements.

Additional vulnerability may arise from, but is not limited to:

- special educational needs or disabilities;
- communication difficulties;
- mental health or emotional needs;
- previous experiences of abuse, neglect or exploitation;
- online or offline bullying;
- social isolation;
- difficulties understanding risk or recognising inappropriate behaviour;
- limited digital literacy;
- family circumstances;
- exploitation or coercion;
- caring responsibilities;
- disadvantage or limited access to appropriate technology;
- language or communication barriers; or
- other individual circumstances identified through safeguarding or pastoral assessment.

The school will take reasonable and proportionate steps to ensure that online learning and safety information is accessible to pupils with additional needs.

This may include:

- accessible digital resources;
- reasonable adjustments to online learning activities;
- alternative methods of communication;
- additional explanation or teaching about online safety;
- increased supervision or support where appropriate;
- adapted reporting mechanisms;
- additional pastoral or safeguarding support; and
- collaboration with parents, carers and relevant professionals where appropriate.

The school will recognise that some pupils may be more susceptible to particular online harms and will consider individual risk as part of safeguarding and online safety assessments.

Online safety education will be age-appropriate, developmentally appropriate and responsive to individual needs.

Pupils will be taught how to:

- recognise unsafe or inappropriate online behaviour;

- protect their personal information;
- manage privacy and security;
- recognise manipulation, coercion and grooming;
- respond to bullying and harmful communication;
- seek help when something online makes them uncomfortable or unsafe; and
- report concerns to a trusted adult or through the school's reporting mechanisms.

The school will provide clear and accessible routes for pupils to report online safety concerns.

Where a pupil has difficulty using standard reporting mechanisms, reasonable alternative arrangements will be provided.

The school will ensure that online safety measures do not unnecessarily exclude pupils from learning opportunities and will balance safeguarding requirements with accessibility, inclusion and educational need.

18. Monitor, Review and Evaluation

The Online School UK will regularly monitor and evaluate the effectiveness of its online safety and acceptable-use arrangements.

Online safety will be treated as a continuing safeguarding and risk-management responsibility rather than a one-off compliance exercise.

The school will monitor, as appropriate:

- online safety incidents and reported concerns;
- safeguarding referrals arising from online activity;
- trends and patterns in online incidents;
- pupil and staff behaviour online;
- compliance with acceptable-use requirements;
- filtering and monitoring alerts and reports;
- unauthorised access attempts and cybersecurity incidents;
- compromised accounts and other security incidents;
- the effectiveness of reporting mechanisms;
- staff online safety training and awareness;
- pupil online safety knowledge and understanding;
- parent and carer engagement;
- accessibility of online safety arrangements;
- emerging technologies and online risks; and
- the effectiveness of controls applied to online teaching and learning.

The DSL will work with relevant school leaders and technical staff to consider safeguarding concerns identified through filtering and monitoring systems and other online safety processes.

The school will ensure that filtering and monitoring arrangements are reviewed for effectiveness at least annually. The review will consider the school's pupil population, risk profile, online provision, devices and systems in use, and any significant changes to technology or safeguarding risks.

Checks of relevant filtering and monitoring arrangements will be undertaken and recorded in accordance with the school's procedures.

Where monitoring, incident analysis or review identifies weaknesses, the school will implement proportionate corrective action and record the action taken.

The school will review this policy:

- at least annually;
- following significant online safety incidents;
- following significant changes to legislation or statutory guidance;
- following significant changes to technology or online learning provision;
- following changes to the school's safeguarding risk profile; and
- where monitoring or evaluation identifies that changes are required.

The review will consider feedback and evidence from, where appropriate:

- pupils;
- parents and carers;
- teaching and support staff;
- the DSL and safeguarding team;
- senior leaders;
- technical or IT personnel;
- governors, proprietors or trustees, where applicable; and
- relevant external agencies or professional advisers.

The outcome of reviews will be used to update this policy, staff training, pupil education, risk assessments, technical controls and other relevant safeguarding arrangements.

Significant findings and actions arising from monitoring and review will be recorded and reported to the appropriate school leadership or governance structure.

The school will ensure that online safety remains integrated with its wider safeguarding, child protection, behaviour, health and safety, data protection and cybersecurity arrangements.