

The Online School UK



Health, Safety and Risk Management 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. First Aid and Medical Emergencies (Pupils and Staff)
3. Risk Management including processes, risk assessment register and scenario risk assessments
4. Online Environment including Filtering and Monitoring and Cyber Security
5. Staff Homeworking
6. Emergency Procedures
7. Monitoring, Training and Review
8. Related Policies and Documents
9. Compliance Framework

1. Introduction

The Online School UK is committed to providing a safe, healthy and supportive educational environment for pupils and a safe working environment for staff.

As an online school, we recognise that our health, safety and risk-management arrangements differ from those of a school operating from a permanent physical site.

Pupils normally access education from their own homes and remain under the care and supervision of their parent/carer when not directly participating in school activities.

The school does not assume responsibility for the physical condition or general safety of a pupil's home. However, the school has a responsibility to identify and manage risks arising from the education and services it provides, including online teaching, safeguarding, supervision, technology, staff working arrangements, foreseeable emergencies and other activities undertaken by or on behalf of the school.

The Online School UK will:

- identify foreseeable health, safety, welfare and safeguarding risks
- assess the likelihood and potential impact of those risks
- implement proportionate control measures
- ensure that significant findings of risk assessments are recorded
- assign responsibility for implementing control measures
- monitor whether controls remain effective
- review risk assessments following incidents, near misses, significant changes or new information
- provide appropriate information, instruction, training and supervision to staff
- maintain appropriate emergency procedures
- maintain appropriate first-aid and medical-emergency arrangements for an online school
- respond appropriately to safeguarding and welfare concerns
- maintain appropriate arrangements for staff working remotely
- maintain appropriate arrangements for online teaching and supervision
- maintain appropriate records
- take action where monitoring identifies deficiencies

This policy forms part of The Online School UK's wider safeguarding, welfare, online safety, data protection, curriculum and operational arrangements. And therefore should be read alongside those policies and procedures.

The school has regard to the Education (Independent School Standards- ISS) Regulations 2014, including:

- Paragraph 7 – safeguarding and welfare of pupils;
- Paragraph 11 – health and safety;

- Paragraph 13 – first aid;
- Paragraph 14 – supervision of pupils;
- Paragraph 16 – risk assessment.

The school also has regard to relevant Department for Education guidance, including the current version of Keeping Children Safe in Education, relevant online safety guidance and health and safety guidance.

The school does not seek to reproduce all requirements of the Independent School Standards within this policy. This policy sets out the arrangements relevant to the school's operating model.

2. First Aid & Medical Emergencies (Pupils and Staff)

First Aid Arrangements

The Online School UK recognises its responsibilities under ISS Paragraph 13, which requires first aid to be administered in a timely and competent manner. As the school operates online and pupils are not physically present on school premises, the school does not provide physical first aid to pupils remotely.

Instead, the school's day to day first-aid arrangements focus on:

- recognising medical emergencies
- obtaining appropriate emergency assistance
- contacting parents/carers
- establishing the pupil's location
- contacting emergency services where necessary
- providing appropriate information to emergency services
- maintaining relevant medical and emergency contact information
- ensuring staff understand their role
- recording incidents
- reviewing arrangements following significant incidents

Staff are not expected or authorised to provide physical first aid remotely or to undertake actions outside their competence.

Emergency procedures must never be delayed while staff attempt to contact the school or complete internal reporting.

Meet-Ups

Where The Online School UK organises or facilitates an in person meet-up, trip, event or other activity where pupils and staff are physically present, additional health, safety, safeguarding and risk-management arrangements will apply.

The school will complete proportionate risk assessments for relevant activities and will consider, as appropriate:

- venue suitability
- supervision
- staff-to-pupil arrangements
- first-aid provision
- emergency procedures
- fire and evacuation arrangements
- accessibility and SEND needs
- medical needs
- safeguarding
- travel arrangements where applicable
- collection and handover arrangements
- behaviour
- missing or separated pupils
- other risks specific to the activity or venue

Where appropriate, the school will obtain relevant information from the venue or activity provider and ensure that staff understand the arrangements before the activity takes place.

The school will not rely solely on the online emergency arrangements in this policy where a physical activity requires different or additional controls.

Medical Information

Before or during admission and throughout a pupil's time at The Online School UK, parents/ carers will have the ability to input appropriate information regarding significant medical conditions, disabilities, allergies and other health needs where this is necessary for the pupil's safety and welfare.

Where appropriate, the school will maintain the following, on a child's student account:

- medical information
- emergency healthcare instructions
- an individual healthcare plan
- emergency contact information
- information supplied by healthcare professionals
- an individual risk assessment

Medical information will be handled securely and in accordance with the school's Data Protection & Information Security Policy.

Where a pupil's medical circumstances change, the school will consider whether existing arrangements and risk assessments require review.

Emergency Contact Information

The Online School UK will maintain appropriate and up-to-date emergency information for every pupil, via the student and parent section on our internal admin panel.

This should include, where appropriate:

- pupil's full name
- home address
- parent/carer name
- primary telephone number
- alternative telephone number
- email address
- relevant medical information
- information about significant medical conditions or allergies
- any other information necessary to enable an emergency response.

The school will take reasonable steps to ensure that this information is kept current.

Parents/carers are expected to notify the school promptly of changes to:

- telephone numbers
- address
- emergency contacts
- medical information
- other information that could affect the school's ability to respond to an emergency.

Establishing the Pupil's Current Location

Because pupils may participate in lessons from different locations, staff must not automatically assume that the pupil is at the home address recorded on the school's system.

Where an emergency occurs during an online lesson, staff must establish the pupil's current physical location where this is necessary to obtain emergency assistance.

Staff should ask the pupil, where possible:

"Where are you right now?"

and, where necessary:

"What is the address where you are?"

Staff should obtain sufficient information for emergency services or a parent/carer to locate the pupil.

Where the pupil is unable to provide their location, staff should use available school records and emergency contact information.

Information concerning the pupil's location should be shared with emergency services where necessary.

Medical Emergency During an Online Lesson

Examples include:

- collapse
- loss of consciousness
- seizure
- serious injury
- significant bleeding
- difficulty breathing
- suspected overdose
- suspected poisoning
- a pupil becoming unresponsive
- suspected serious medical episode
- any other situation where there is an immediate concern for the pupil's life or physical safety

The staff present in a lesson should:

1. remain calm
2. maintain communication with the pupil where possible
3. establish whether the pupil is responsive
4. establish the pupil's current physical location
5. establish whether a parent/carer or responsible adult is present
6. contact emergency services where appropriate
7. provide the emergency operator with the pupil's location
8. provide relevant factual information
9. contact the parent/carer where appropriate
10. inform the DSL or DDSL
11. remain connected with the pupil where safe and appropriate
12. follow emergency-service instructions
13. record the incident once the immediate emergency has been addressed

For teachers, we recognise their need to gain assistance from the Happiness Manager in lessons with them, in order to establish the pupil's current location and/or home address. This should be done alongside the above steps, not delaying the need for emergency assistance.

Calling 999 takes priority over contacting the school, parent/carer or DSL where immediate emergency assistance is required.

Parent/Carer presence

Where a parent/carer or another responsible adult is present, staff in lessons should encourage them to provide appropriate immediate assistance and contact emergency services where necessary.

Staff should still provide factual information and follow emergency-service instructions as the presence of a parent/carer does **not** prevent the school from taking appropriate safeguarding action where a safeguarding concern exists.

If a Parent/Carer cannot be contacted

Where a pupil appears to be experiencing an emergency and a parent/carer cannot be contacted by the school:

- emergency services should be contacted where appropriate
- the DSL or senior leadership should be informed
- alternative emergency contacts may be contacted where appropriate
- emergency services should be provided with the pupil's known location and relevant information
- the school should continue reasonable attempts to contact the parent/carer
- all actions and attempted contacts should be recorded via the schools internal safeguarding panel

If a pupil disconnects during an apparent medical, welfare or safeguarding emergency, staff must not assume that the situation has been resolved.

Depending on the circumstances, staff should:

- attempt to reconnect
- contact the pupil using an approved school method
- contact the parent/carer
- contact emergency services where there is a reasonable concern for immediate safety
- inform the DSL or senior leader
- record the actions taken.

Staff Medical Emergencies

Staff working remotely should take reasonable steps to protect their own health and safety.

Where a staff member becomes seriously unwell while working, they should contact emergency services where necessary and notify an appropriate colleague or manager as soon as reasonably practicable. This may be done via WhatsApp, Slack or Email.

The Online School UK will maintain arrangements for:

- lesson cover
- safeguarding escalation
- management contact
- pupil welfare
- recording significant incidents

First-Aid and Emergency Training

The school will ensure that relevant staff understand the school's online medical-emergency procedures. This includes teachers, Happiness Manager Assistants and Happiness Manager Leads- as the individuals in lessons with pupils.

Training and induction will cover, as appropriate:

- recognising an emergency
- emergency escalation
- contacting 999
- obtaining a pupil's location
- contacting parents/carers
- safeguarding escalation
- recording incidents
- staff responsibilities and limitations

The DSL will assess, on an ongoing basis, whether additional training is appropriate based on its pupil population and identified risks.

3. Risk Management & Risk Assessment

Risk Assessment Framework

The Online School UK maintains a systematic approach to identifying, assessing and controlling risks.

This section supports ISS Paragraph 16.

The school will identify risks associated with:

- online teaching
- safeguarding
- pupil welfare
- supervision
- emergency situations
- staff homeworking
- lone working
- technology and cybersecurity
- online communication
- attendance and pupil engagement
- individual pupil circumstances
- educational activities
- equipment and systems
- other foreseeable activities or circumstances.

Health and safety risk assessments will consider risks to employees and other persons who may be affected by the school's activities. The school will record significant findings and identify appropriate control measures.

Individual risk assessments are available upon request.

Responsibilities

The Director has overall responsibility for ensuring that the school has appropriate health, safety and risk-management arrangements.

The Headteacher is responsible for implementing and monitoring this policy and ensuring that appropriate risk assessments are completed.

The CEO has overall responsibility for ensuring appropriate health, safety and risk-management arrangements. The Headteacher is responsible for operational implementation and monitoring. The DSL is responsible for safeguarding-related risk management and escalation within their safeguarding role.

All staff at The Online School UK are responsible for:

- following risk controls
- reporting hazards

- reporting incidents and near misses
- participating in relevant risk assessments
- completing required training
- informing leaders where controls appear ineffective

Risk Assessment Process

Risk assessments should identify:

1. the activity, situation or hazard
2. who may be affected
3. existing control measures
4. likelihood
5. potential severity/impact
6. overall level of risk
7. additional controls required
8. person responsible for implementing controls
9. timescale for action
10. date of assessment
11. review date
12. evidence that required actions have been completed

Risk assessments should be proportionate to the level of risk.

Risk Assessment Register

The Online School school will maintain a Risk Assessment Register identifying its principal current risk assessments.

The register should record:

- assessment title
- assessment owner
- date completed
- date reviewed
- current risk rating
- actions outstanding
- responsible person
- next review date

The Risk Assessment Register is an internal management document , handled by the Director, Headteacher and DSL.

Scenario Risk Assessments

The Online School UK maintain separate assessments for significant scenarios where appropriate, where potential risks could be identified. These are internal operational documents, handled by the Director, Headteacher and DSL. Reviewed annually and/ or after an incident or near miss.

Examples include:

Online Teaching Risk Assessment

May consider:

- one-to-one lessons
- professional boundaries
- online communication
- webcam use
- screen sharing
- recording
- inappropriate content
- unauthorised participants
- interruptions
- loss of communication
- supervision

Online Safeguarding Risk Assessment

May consider:

- online grooming
- exploitation
- inappropriate messaging
- child-on-child abuse
- harmful content
- webcam misuse
- inappropriate contact
- online radicalisation
- cyberbullying
- safeguarding concerns identified through technology

Emergency During Online Lesson Risk Assessment

May consider:

- medical emergencies
- safeguarding emergencies
- loss of communication
- pupil location
- emergency contact information
- parent/carer contact
- emergency services
- escalation
- incident recording

Staff Homeworking Risk Assessment

May consider:

- workstation safety
- DSE- Display Screen Equipment
- electrical equipment
- work-related stress
- lone working
- confidentiality
- emergency arrangements
- working environment

IT and Cybersecurity Risk Assessment

May consider:

- hacking
- account compromise
- malware
- data breaches
- loss of systems
- platform failure
- unauthorised access
- cyber incidents

Individual Pupil Risk Assessments

An individual pupil risk assessment **may** be completed where a pupil has an identified risk requiring additional or individual controls.

This may arise from:

- safeguarding concerns
- medical needs
- SEND
- mental health or wellbeing
- behavioural risks
- vulnerability
- online safety concerns
- attendance concerns
- exploitation
- serious violence concerns
- other individual circumstances

The assessment should identify:

- the specific risk
- circumstances in which the risk may arise
- who may be affected
- existing controls
- additional controls
- responsible staff
- information that relevant staff need to know
- review arrangements
- escalation arrangement

Individual pupil risk assessments are confidential. Access is restricted to those who need the information to implement the identified controls, which may include:

- DSL
- Headteacher
- relevant senior leaders
- relevant teachers
- SEND Lead
- HMLs
- HMAs
- appropriate external professionals
- parents/carers where appropriate.

An individual pupil risk assessment does not replace safeguarding records, healthcare plans or other statutory records.

Where the assessment relates to safeguarding, the DSL must ensure that the safeguarding concern, decisions, actions, rationale and outcomes are recorded through the school's safeguarding recording system.

Risk Controls

The Online School UK will seek to eliminate risks wherever reasonably practicable and otherwise reduce them to an acceptable level.

Controls may include:

- policies
- procedures
- staff training
- supervision
- technical controls
- filtering and monitoring
- access controls
- parental involvement
- emergency procedures
- individual support
- additional staffing
- monitoring
- equipment or system changes
- specialist advice

Review of Risk Assessments

Risk assessments will be reviewed:

- at planned intervals
- following an accident
- following a near miss
- following a safeguarding incident
- following a significant change
- when new technology or systems are introduced
- when a new activity is introduced
- where controls are ineffective
- following relevant legislative or guidance changes
- whenever new information indicates that the assessment should be reconsidered

Where significant actions are identified, these will be assigned to an appropriate person and monitored through to completion. This individual is likely the Headteacher or DSL.

4. Online Environment

Safe Use of Technology

The Online School UK recognises that its online environment forms part of the educational environment.

The school will maintain arrangements for:

- safe online teaching
- appropriate professional communication
- online safeguarding
- filtering and monitoring
- cybersecurity
- data protection
- acceptable use
- reporting online incidents
- managing harmful or inappropriate content
- preventing unauthorised access
- responding to safeguarding concerns

These arrangements support ISS Paragraphs 7, 14 and 16.

This section of the policy should be read alongside the schools Safeguarding and Child Protection Policy, Online Safety Policy, Staff Communication and Conduct Policy, Safer Recruitment Policy and Filtering and Monitoring Policy,

Online Teaching and Supervision

The Online School UK recognises that online and remote learning creates safeguarding, health, safety, privacy, cybersecurity and professional-boundary risks that may differ from those present in a physical school environment.

Online teaching and supervision must therefore be planned and delivered in a manner that protects pupils and staff and is consistent with the school's safeguarding, child protection, online safety, acceptable-use, staff conduct, data protection and information security requirements.

The level and nature of supervision and control applied to online teaching will be proportionate to:

- the age and developmental stage of pupils
- individual needs and vulnerabilities
- identified safeguarding and risk factors
- the nature and content of the lesson or activity
- whether teaching is delivered individually or to a group
- group size and composition

- the platform, application or technology being used
- whether the activity is live, recorded or asynchronous
- the location and circumstances from which pupils and staff are participating

Online teaching must not be treated as a lower-risk alternative to face-to-face teaching. Safeguarding responsibilities apply equally when pupils are learning remotely.

One-to-One Online Teaching and Supervision

One-to-one online teaching, tutoring, mentoring, pastoral support or other direct online contact with a pupil must be undertaken in accordance with the school's safeguarding and online-working procedures.

Staff must:

- use only school-approved platforms, accounts and communication channels;
- use school-managed accounts wherever provided;
- maintain appropriate professional boundaries at all times;
- communicate with pupils only through approved school channels and within agreed arrangements;
- not use personal social-media accounts, personal messaging services or unapproved communication platforms to communicate privately with pupils;
- ensure that one-to-one online contact is appropriately authorised and capable of being subject to safeguarding oversight;
- maintain appropriate records of significant meetings, concerns, disclosures or safeguarding incidents;
- report safeguarding concerns in accordance with the school's safeguarding and child protection procedures; and
- report any concern about their own conduct, another adult's conduct or a potential boundary issue through the school's established safeguarding or low-level concerns procedures.

Where appropriate and proportionate to the circumstances, the school may require additional safeguards for one-to-one online contact, including parental/carers awareness or involvement, additional staff oversight, use of a second adult, or alternative arrangements.

One-to-one online contact must not be used to circumvent the school's safeguarding, communication or supervision arrangements.

Online Lesson Security and Authorised Participants

Online lessons and meetings must be configured to minimise the risk of unauthorised access or inappropriate interaction.

Where supported by the platform, staff should use appropriate security controls, including:

- authenticated school accounts
- unique or controlled meeting links
- passwords or equivalent access controls
- waiting rooms or equivalent admission controls
- restrictions on screen sharing, file sharing, chat and other participant functions where appropriate
- appropriate host and participant permissions
- controls that allow staff to mute, remove or otherwise restrict participants where necessary

Online lessons must only be accessed by authorised participants.

Where a teacher becomes aware of an unknown, unauthorised or unexpected participant, the teacher should take immediate reasonable steps to secure the session, including removing or restricting the participant where possible. The incident must be reported in accordance with the school's incident-reporting procedures and referred to the DSL where there is a safeguarding concern.

Relevant evidence should be preserved where appropriate and lawful to do so.

Webcam, Camera and Home Environment Safety

The school will take reasonable steps to ensure that the use of cameras does not unnecessarily expose pupils or staff to privacy or safeguarding risks.

Where cameras are used:

- staff should use an appropriate professional or neutral background where reasonably practicable
- staff should avoid displaying personal, confidential or sensitive information
- staff should avoid using private spaces such as bedrooms for online teaching wherever reasonably practicable
- pupils should not normally be required to reveal unnecessary information about their home, family or personal circumstances
- staff should consider the potential safeguarding implications of what is visible or audible within the online environment
- pupils should be provided with clear expectations regarding appropriate camera use, dress, behaviour and backgrounds

- staff should respond appropriately where concerning, inappropriate or potentially unsafe content is visible or audible
- concerns about the presence of an unauthorised adult or other person in the pupil's environment should be considered in accordance with safeguarding procedures
- reasonable adjustments should be considered for pupils whose individual circumstances make camera use inappropriate, distressing or inaccessible

Camera use must not be used in a way that unnecessarily intrudes upon the privacy or dignity of pupils or staff.

Online Behaviour and Professional Boundaries

The school's expectations for behaviour, respect, anti-bullying, safeguarding and professional conduct apply equally to online learning.

Staff and pupils must not use online lessons, chats, messaging functions or associated digital platforms to engage in:

- bullying or cyberbullying
- harassment or sexual harassment
- discriminatory or prejudicial behaviour
- threatening or abusive communications
- inappropriate sexualised communication
- sharing of inappropriate or harmful material
- unauthorised sharing of images, recordings or personal information
- grooming or other inappropriate contact
- harmful or abusive behaviour towards other pupils
- behaviour that could place themselves or another person at risk of harm

The school recognises that online child-on-child abuse can include cyberbullying, harassment, harmful sexual behaviour, sexual harassment, the non-consensual sharing of intimate images and other harmful online interactions. Such behaviour will be treated as a safeguarding matter and managed in accordance with the school's safeguarding and child protection procedures.

Recording, Screenshots and Digital Capture

Online lessons, meetings or activities must not be recorded, photographed, screenshotted or otherwise captured unless this is authorised by the school and undertaken in accordance with the school's policies and applicable data protection requirements.

Where recording is authorised, the school must establish, as appropriate:

- the purpose and lawful basis for recording
- who is authorised to make the recording
- who may access the recording
- how the recording will be stored and secured
- the applicable retention period
- how the recording will be securely deleted when no longer required

Staff and pupils must not make unauthorised recordings, screenshots, photographs or other digital captures of online lessons or other participants.

Any suspected misuse, unauthorised recording or inappropriate sharing of recorded material must be reported through the school's established procedures.

Filtering and Monitoring

The school will maintain appropriate filtering and monitoring arrangements to help protect pupils from illegal, inappropriate and harmful online content and activity.

Filtering and monitoring arrangements will be proportionate to the school's risk profile and will take account of:

- the age and number of pupils
- the needs and vulnerabilities of individual pupils
- the devices, platforms and services used
- the locations from which pupils access online provision
- the nature and extent of online activity;
- emerging online risks

The school will:

- assign clear responsibility for the management of filtering and monitoring
- maintain appropriate filtering and monitoring systems
- ensure that systems are appropriately configured and maintained
- undertake and record a review of filtering and monitoring effectiveness at least annually
- undertake appropriate checks across relevant internet-connected devices and services
- ensure relevant staff understand the filtering and monitoring arrangements and how to escalate concerns
- respond promptly to alerts or identified safeguarding concerns
- investigate significant incidents where appropriate
- involve the DSL where filtering or monitoring identifies a safeguarding concern

The school recognises that filtering and monitoring cannot eliminate all online risk. Technical controls therefore form one part of the school's wider safeguarding, education, supervision and risk-management arrangements.

Filtering must not unreasonably restrict appropriate teaching and learning.

Cybersecurity and Information Security

The school will maintain appropriate technical and organisational measures to reduce cybersecurity and information-security risks associated with online teaching.

Depending on the school's risk assessment and technical environment, these measures may include:

- secure authentication
- strong and unique passwords
- multi-factor authentication where appropriate
- role-based access controls
- appropriate account permissions
- secure school-managed device
- software and security updates
- malware and endpoint protection
- secure networks and connections
- data backup and recovery arrangements
- staff awareness and cybersecurity training
- appropriate management of third-party applications and services
- incident-response and business-continuity arrangements

Staff must follow the school's Data Protection and Information Security Policy and must report suspected compromised accounts, phishing, malware, data loss, data breaches or other cybersecurity incidents promptly through the school's established procedures. This can be found via the TOS Policies section on our school website.

Online Safeguarding Risks

The Online School UK recognises that online safeguarding risks may include, but are not limited to:

- exposure to illegal, inappropriate or harmful content
- pornography and sexually explicit material
- online sexual abuse, grooming and exploitation
- cyberbullying and harassment
- sexual harassment and harmful sexual behaviour
- non-consensual sharing of intimate images
- AI-generated or digitally manipulated sexual or harmful content
- harmful or abusive communications

- misogynistic, discriminatory, racist or extremist content
- radicalisation and exposure to extremist material
- harmful online challenges
- inappropriate contact with adults or other users
- impersonation and identity-related risks
- phishing, scams and financial exploitation
- compromised accounts
- inappropriate use of artificial intelligence
- loss or unauthorised disclosure of personal data
- other emerging online harms

The school will keep its assessment of online risks under review as technology, platforms and patterns of online harm develop.

Reporting and Responding to Online Incidents

Staff must report online safeguarding or safety concerns promptly through the school's established reporting procedures.

Reportable incidents include, but are not limited to:

- suspected grooming or online sexual exploitation
- harmful or illegal online content
- cyberbullying
- sexual harassment or harmful sexual behaviour
- harmful or threatening communications
- non-consensual sharing of intimate images
- concerning AI-generated or manipulated content
- suspected radicalisation or extremist content
- compromised accounts
- suspected cybercrime, phishing or scams
- data breaches or loss of personal information
- inappropriate use of technology or online platforms
- unauthorised participants
- unauthorised recording or screenshots
- concerns arising from a pupil's online environment
- any other online incident that may place a pupil or member of staff at risk

Where an incident presents a safeguarding concern, the DSL must be informed without delay and the school's safeguarding and child protection procedures must be followed.

Where an incident involves a concern about the conduct of a member of staff, the school's procedures for allegations, concerns about staff and low-level concerns must also be followed as appropriate.

The school will ensure that online incidents are recorded, investigated and escalated proportionately to the level of risk and in accordance with applicable safeguarding, data protection and information-security requirements.

Online Safety Education

The school will ensure that pupils are provided with age- and developmentally appropriate opportunities to understand online risks and how to seek help.

Online safety education will address relevant risks associated with content, contact, conduct and commerce and will be integrated into the school's wider safeguarding and curriculum arrangements.

Pupils will be provided with clear, accessible and child-friendly mechanisms for reporting online concerns and seeking support.

Parents and carers will be provided, where appropriate, with clear information about online learning arrangements, including the platforms and services pupils are expected to use and the nature of online interaction with school staff and other pupils.

Review and Risk Management

The school will review its online teaching and supervision arrangements regularly and following significant incidents, changes in technology, changes in the school's provision or changes in the risk profile of pupils.

Online safeguarding arrangements will form part of the school's wider safeguarding and risk-management framework and will be reviewed alongside the school's Online Safety Policy, Child Protection and Safeguarding Policy, Staff Communication and Conduct Policy, Data Protection and Information Security Policy, Acceptable Use Policy and relevant risk assessments.

5. Staff Homeworking

As an online school, staff will work remotely from their home place or designated workplace.

Staff therefore remain responsible for taking reasonable steps to maintain a safe working environment within their control.

The Online School UK does not control or assume responsibility for the general condition of an employee's home.

However, the school will provide appropriate guidance concerning the following, as outlined through this policy:

- safe working practices
- display screen equipment
- workstation arrangements
- electrical safety
- work-related stress
- lone working
- confidentiality
- cybersecurity
- incident reporting

Workstation and DSE Assessments

Staff who regularly use display screen equipment (DSE) will be expected to:

- position screens appropriately
- maintain suitable posture
- take appropriate breaks
- vary activities
- report discomfort
- report equipment problems
- request reasonable adjustments where necessary

Electrical Safety

All staff should use electrical equipment safely when working for The Online School UK.

Staff must:

- avoid overloaded socket;
- maintain cables safely
- remove damaged equipment from use
- follow manufacturer instructions
- report school-owned equipment concerns
- not use equipment they reasonably believe to be unsafe

Work-Related Stress and Lone Working

The Online School UK recognises the potential for remote working to contribute to work-related stress, including the factor of lone working.

The Online School UK will seek to:

- maintain reasonable workloads
- provide management support
- encourage appropriate breaks
- maintain communication
- monitor staff wellbeing
- identify work-related stress risks
- consider reasonable adjustments where appropriate

Staff are regularly made aware of their right and ability to speak to our in house Mental Health Practitioner should they feel affected or at risk of suffering work related stress. In addition to partaking in weekly meetings which vary in agenda and all have the same aim as to support staff in some way. These meetings include but are not limited to: Department meetings, wellbeing and mental health focus, staff social events.

Confidentiality

All staff who work for or are in association with The Online School UK must protect pupil, parent and school information while working remotely.

This includes:

- preventing unauthorised viewing of information on devices
 - using approved devices
 - using approved communication systems (Slack, Email, private chats, email)
 - locking devices when unattended
 - avoiding confidential conversations
 - following our Data Protection & Information Security Policy
-

6. Emergency Procedures

Emergency Response Principles

The Online School UK maintains emergency response procedures appropriate to its online operating model.

Emergency procedures are designed to ensure that the school can respond promptly and proportionately to foreseeable emergencies which may affect pupils, staff, the delivery of education or the school's ability to operate safely.

Emergency responses will prioritise:

1. immediate safety
2. contacting emergency services where necessary
3. safeguarding and welfare
4. appropriate parent/carers contact
5. school escalation
6. maintaining continuity of education where reasonably practicable
7. accurate recording, review and learning from the incident

Staff must not allow internal reporting requirements to delay emergency assistance.

Medical emergencies involving a pupil or staff member are addressed under Section 2: First Aid & Medical Emergencies.

Safeguarding Emergencies

Where an emergency presents an immediate safeguarding concern, staff must follow the school's Safeguarding and Child Protection Policy and inform the DSL without delay.

Where the DSL is unavailable, staff must follow the school's DDSL or senior-leadership escalation arrangements.

Where immediate action is required to protect a child, staff should contact the appropriate emergency service or safeguarding authority directly in accordance with the school's safeguarding procedures.

The school's safeguarding procedures take priority where an emergency involves an immediate risk of harm to a child.

Loss of Communication With a Pupil

Where communication is unexpectedly lost during a situation giving rise to reasonable concern for a pupil's immediate safety, staff must consider the circumstances and take proportionate action.

This may include:

- attempting to reconnect with the pupil

- contacting the pupil using an approved school communication method
- contacting the parent/carer
- using available emergency contact information
- contacting emergency services where there is a reasonable concern for immediate safety
- notifying the DSL or senior leader
- recording the actions taken

Where the circumstances indicate an immediate medical emergency, staff must follow the procedure in Section 2.

Serious Technology or Cybersecurity Emergencies

The school recognises that, as an online school, significant technology or cybersecurity incidents may affect the school's ability to safely deliver education.

Examples include:

- significant platform failure
- loss of access to critical systems
- widespread loss of communication
- major cybersecurity incident
- ransomware or malware affecting critical systems
- significant data breach
- compromise of staff or administrator accounts
- another technology incident that creates a significant safeguarding, welfare or operational risk

The school will maintain appropriate contingency arrangements for significant technology incidents.

Where appropriate, these may include:

- notifying relevant senior leaders
- contacting the relevant technology provider
- activating alternative communication arrangements
- using alternative teaching arrangements
- assessing safeguarding implications
- assessing data-protection implications
- informing the DSL where pupils may be affected
- informing the Data Protection Lead or appropriate senior leader where a data breach may have occurred
- maintaining appropriate records
- reviewing the incident afterwards

Further details are contained within the Data Protection & Information Security Policy, Online Safety Policy and relevant IT/Cybersecurity Risk Assessment.

Staff Incapacity

Where a staff member becomes unexpectedly unavailable or incapacitated during the delivery of an online lesson or other school activity, the school will take reasonable steps to ensure:

- pupil welfare;
- appropriate lesson cover;
- safeguarding escalation where necessary;
- appropriate parent/carer communication where required;
- management notification; and
- recording of any significant incident.

Where a staff member becomes medically unwell, the First Aid & Medical Emergencies procedures in Section 2 apply.

Other Foreseeable Emergencies

The school will identify and assess other foreseeable emergencies through its risk-management process.

Where a particular emergency presents a significant risk, the school will maintain an appropriate procedure or contingency arrangement.

Relevant risks may include:

- significant loss of technology
- loss of communication systems
- cybersecurity incidents
- serious safeguarding incidents
- staff incapacity
- loss of contact with a vulnerable pupil
- disruption to critical school systems
- other emergencies identified through the school's risk assessments

Specific procedures will be maintained separately where necessary and referenced through the school's Risk Assessment Register.

Emergency Procedure Testing

The school will periodically test or review its emergency arrangements to ensure that they remain workable and appropriate to its operating model.

Testing **may** include:

- scenario-based exercises
- tabletop exercises
- staff briefings/ refresher courses
- testing emergency contact arrangements
- testing pupil-location procedures
- testing alternative communication arrangements
- reviewing technology-contingency arrangements
- reviewing procedures following an actual incident

The school will record significant findings and make improvements where required.

Incident Recording and Review

Significant emergencies must be recorded through the school's internal safeguarding panel, using the appropriate label "Health and Safety Emergency".

Records should include, where appropriate:

- date and time
- nature of the emergency
- persons affected
- actions taken
- emergency services contacted
- parent/carer contact
- DSL or senior leader notification
- systems or services affected
- outcome
- further action required
- review undertaken

Personal, safeguarding and other confidential information must be stored securely.

Following a significant emergency, the school will consider whether:

- existing controls were effective
- staff followed the relevant procedure
- additional training is required
- a risk assessment requires amendment

- a procedure requires amendment
 - further safeguarding, health and safety or data-protection action is required.
-

7. Monitoring, Training & Review

The school will ensure that staff receive appropriate information relevant to their responsibilities.

This will be done via three methods: DSL led training, refresher training courses and policy reading. On areas such as:

- health and safety
- emergency procedures
- online teaching safety
- Safeguarding and child protection
- online safety
- first-aid/emergency arrangements
- data protection
- cybersecurity
- DSE/homeworking
- lone working
- risk assessments
- incident reporting

Training will be refreshed where necessary via refresher courses held throughout the academic year, following significant changes to procedures and/or after an incident or near miss.

Training records will be maintained by the DSL on The Online School UK's Safeguarding Training Log.

Monitoring

The school will monitor the effectiveness of its arrangements through:

- risk assessment reviews
- Incident and accident records via the internal safeguarding panel
- near-miss records
- safeguarding records
- online incident records
- filtering and monitoring reviews
- staff feedback;
- pupil/parent feedback where appropriate;

- staff training records;
- review of emergency procedures;
- review of individual risk assessments; and
- management review.

Accidents, Incidents and Near Misses

Staff must report accidents, significant incidents and near misses through the school's internal safeguarding panel, using the appropriate label "Health and Safety Emergency".

The school will consider whether each significant incident indicates:

- a new risk
- an inadequately controlled existing risk
- a training requirement
- a procedural weakness
- a safeguarding concern
- a need to amend a risk assessment

Review Following Significant Events

Following a significant incident, the school will consider:

- what happened
- whether the response was timely and appropriate
- whether existing controls were effective
- whether staff followed procedures
- whether further action is required
- whether training is required
- whether a risk assessment needs to be amended
- whether a policy or procedure requires review

Evidence and Record Keeping

The school will retain appropriate evidence demonstrating that its health, safety and risk-management arrangements are implemented.

Evidence may include:

- current policies;
- risk assessments;
- Risk Assessment Register;
- review records;
- action logs;
- staff training records;
- DSE assessments;
- incident and accident records;
- emergency exercise records;
- individual pupil risk assessments;
- relevant medical/healthcare arrangements;
- equipment or system checks;
- online safety records; and
- records of actions taken following identified risks.

Records will be retained and managed in accordance with the school's Data Protection & Information Security Policy and relevant retention requirements.

Policy Review

This policy will normally be reviewed at least annually.

It will also be reviewed sooner where:

- legislation or statutory guidance changes
- the school's operating model changes
- a significant risk is identified
- a serious incident occurs
- an inspection identifies an area requiring improvement
- an emergency procedure is found to be ineffective
- existing arrangements require amendment

The CEO will ensure that the policy remains current and that significant changes are communicated to relevant staff.

8. Related Policies and Documents

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Filtering and Monitoring Policy

- Data Protection & Information Security Policy
- Staff Communication and Conduct Policy
- Behaviour Policy
- Attendance Policy
- SEND Policy
- Equality, Diversity & Inclusion Policy
- Acceptable Use Policy
- Complaints Policy
- Staff Homeworking Risk Assessment
- Lone Working Risk Assessment
- Online Teaching Risk Assessment
- Online Safeguarding Risk Assessment
- Emergency During Online Lesson Risk Assessment
- IT & Cybersecurity Risk Assessment
- Risk Assessment Register
- Individual Pupil Risk Assessments
- Individual Healthcare Plans where applicable

9. Compliance Framework

This policy contributes to the school's arrangements for meeting the following requirements:

Requirement	Relevant sections
ISS 7 – Safeguarding and welfare	Sections 2, 3, 4 and 6
ISS 11 – Health and safety	Sections 1, 3, 5, 6 and 7
ISS 13 – First aid	Section 2
ISS 14 – Supervision	Sections 2, 4 and 6
ISS 16 – Risk assessment	Section 3

KCSIE 2026 – safeguarding arrangements	Sections 2, 3, 4 and 6
--	------------------------

Online safeguarding	Section 4
---------------------	-----------

Filtering and monitoring	Section 4.6
--------------------------	-------------

Cybersecurity	Section 4.7
---------------	-------------

Emergency response	Sections 2 and 6
--------------------	------------------

Staff health and safety	Section 5
-------------------------	-----------

Risk assessment monitoring	Sections 3 and 7
----------------------------	------------------

Incident and near-miss review	Section 7
-------------------------------	-----------

This policy is one component of the school's overall compliance arrangements. Compliance depends upon the effective implementation, monitoring, recording and review of the procedures and controls described within this policy and its supporting documents.