CASSIOBURY INFANT & NURSERY SCHOOL

Online Safety & Data Security Policy

Author	HfL model policy
Date	September 2026
Adopted by	FGB
Review period	Annually
Date of last Review	September 2025
Date of Next Review	September 2027

Contents

- 1. Purpose and principles
- 2. Responsibilities and governance
- 3. Scope
- 4. Online safety and safeguarding
- 5. Filtering and monitoring
- 6. Artificial intelligence (AI)
- 7. Cyber security, information security and access management
- 8. Email, messaging and online communication
- 9. Websites, apps, downloading and online services
- 10. Images, video and personal data
- 11. Mobile phones and personal devices
- 12. New technology, remote learning and off-site provision
- 13. Reporting, responding to and recording incidents
- 14. Curriculum and digital literacy
- 15. Staff, governor and volunteer training
- 16. Working with parents and carers
- 17. Monitoring, review and assurance
- Appendix 1 – Online safety incident record
- Appendix 2 – Annual filtering and monitoring assurance record

Policy note: This document has been updated for September 2026. It reflects the final Keeping Children Safe in Education 2026, current DfE filtering and monitoring guidance, current DfE digital and technology standards, and Ofsted inspection arrangements applying from September 2026. It does not replace the school's wider safeguarding or data protection policies.

1. Purpose and principles

Cassiobury Infant & Nursery School recognises that internet, mobile and digital technologies are an important part of children's learning, communication and everyday lives. They also create safeguarding, privacy, wellbeing, cyber security and reputational risks. The school therefore treats online safety as an integral part of safeguarding, rather than as a separate technical issue.

The school will provide a safe, supportive and developmentally appropriate digital environment in which pupils can learn how to use technology safely, responsibly and critically. Online safety will be embedded across safeguarding, curriculum, staff training, filtering and monitoring, behaviour, mobile phone arrangements, data protection and engagement with parents and carers.

The school recognises that some pupils may be at increased risk of online harm because of age, SEND, communication or developmental needs, additional vulnerabilities or individual circumstances. Online safety teaching, supervision, filtering, monitoring and safeguarding responses will be adapted where necessary to meet individual needs.

The school will follow a child-centred approach. Where online activity raises a safeguarding concern, the school's child protection procedures take precedence over this policy and concerns will be referred to the DSL without delay.

The school will consider the four areas of online risk: content, contact, conduct and commerce. These risks may include harmful or illegal content; grooming and exploitation; bullying and harmful behaviour; sharing or creation of sexualised images, including AI-generated images; scams, phishing and inappropriate commercial activity; misinformation, disinformation and conspiracy theories; extremism; and other emerging online harms.

2. Responsibilities and governance

The Headteacher and governing body have ultimate responsibility for ensuring that effective online safety arrangements are in place, implemented and monitored. The designated online safety lead is Mrs Charlotte Cooper, who is also the school's DSL as identified in the Child Protection and Safeguarding Policy.

The governing body will seek assurance that online safety is part of the school's whole-school safeguarding approach and that leaders can demonstrate how pupils are taught to stay safe online and how the school's information systems safeguard pupils from online harm. This includes oversight of filtering and monitoring, cyber security, policy review, staff training, incident trends and actions arising from reviews.

The SLT member responsible for filtering and monitoring Mrs Charlotte Cooper who is also the school's DSL and will liaise with the IT support/provider to ensure systems are effective, appropriately configured and reviewed. Where responsibilities are delegated, the school will retain clear accountability and records of checks and actions.

All staff, governors, volunteers, contractors and visitors have a responsibility to follow this policy and report concerns promptly. Staff must not investigate safeguarding concerns themselves or delay reporting while attempting to establish the facts.

Any organisation using school premises must follow its own arrangements where it is genuinely independent of the school. However, where it has access to school systems, equipment, pupils or school activities, it must comply with relevant school safeguarding, online safety and acceptable use requirements.

3. Scope

This policy applies to:

• pupils; • parents and carers; • teaching and support staff;	• school governors; • peripatetic teachers, coaches, supply teachers and student teachers; • visitors and volunteers;	• contractors and other professionals working with pupils; • organisations using school facilities where the school's safeguarding arrangements apply; • pupils receiving education off site, on trips, or through remote learning arrangements.

The school expects appropriate online behaviour both on and off the school site where conduct affects the safety, wellbeing or education of pupils or staff, or creates a safeguarding concern.

4. Online safety and safeguarding

Online safety is a running and interrelated theme within the school's safeguarding arrangements. It will be reflected in the Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, curriculum planning, staff training, parental engagement and risk assessments.

The school will consider online harms in individual safeguarding assessments, including where a child is being groomed, bullied, exploited, exposed to harmful content, pressured to share images or information, or affected by harmful online communities or communications.

Online harms may occur away from school and on devices or networks not controlled by the school. The school will respond where information comes to its attention and where safeguarding, behaviour or welfare responsibilities are engaged, working with parents/carers and external agencies where appropriate.

The school will consider the needs of pupils with SEND and other vulnerabilities when assessing online risk, teaching online safety and deciding on reasonable adjustments or additional supervision.

5. Filtering and monitoring

The school will maintain appropriate filtering and monitoring systems to protect pupils from illegal, inappropriate and potentially harmful online content and activity. Filtering is preventative; monitoring is reactive and may identify activity that requires review or safeguarding action.

School-specific systems must be recorded and kept current. The following local information must be completed and reviewed by the school:

- Filtering provider/system: RM
- Monitoring provider/system: RM
- IT support/provider: Con-Ed
- DSL for filtering and monitoring: Mrs Charlotte Cooper
- Governance oversight: governing body

The DSL and IT support/provider will:

- ensure filtering and monitoring are operational and appropriately configured;
- ensure filtering applies to relevant school-managed internet-connected devices and networks and is checked in all relevant locations;
- ensure safe-search and other appropriate safety settings are enabled;
- ensure systems can identify users where necessary so that concerns can be traced to individuals;
- ensure staff know what is filtered/monitored, how alerts are generated and how concerns are escalated;
- review monitoring alerts and reports promptly and refer safeguarding concerns to the DSL;
- ensure temporary exceptions to filtering or monitoring are authorised, documented and risk assessed;
- assess new devices, applications, platforms and online services before use, including safeguarding, data protection, age appropriateness and filtering/monitoring implications;
- restrict access to monitoring data to authorised staff and ensure appropriate retention arrangements;
- keep records of checks, concerns, actions and outcomes.

The effectiveness of filtering and monitoring will be reviewed and checked at least once in every academic year. The annual review will include checks that filtering is working appropriately on all relevant internet-connected devices and in all

relevant locations, with a written record of the checks, findings, actions and completion dates. The review will also consider pupil age, vulnerabilities, emerging online risks and the effectiveness of monitoring.
A further review will take place following a significant safeguarding incident, significant technology change, introduction of a new digital system, or other material change in risk.
The school will consider DfE digital and technology standards when reviewing provision and will use relevant DfE self-assessment resources where appropriate. The school will also ensure that filtering and monitoring arrangements are reflected in privacy information, data protection arrangements and staff training.

6. Artificial intelligence (AI)

The school recognises that generative AI can provide educational opportunities but can also create safeguarding, data protection, privacy, ethical, intellectual property and misinformation risks. AI-generated content may include harmful or sexualised images, deepfakes, false information or content designed to manipulate or exploit children.
The school will:

- approve AI tools before they are used with or by pupils, considering age appropriateness, safeguarding, data protection, filtering/monitoring and educational purpose;
- not permit staff to enter personal, confidential or sensitive information about pupils, families or staff into unapproved AI tools;
- consider whether AI systems can generate, recommend or expose children to harmful content and whether safety controls are adequate;
- provide staff with appropriate guidance on safe and responsible AI use;
- teach pupils, at an age-appropriate level, that AI can create content that is inaccurate, misleading or not real, and how to seek help when something online causes concern;
- respond to AI-generated bullying, sexualised images, impersonation, deepfakes or other harmful material as a safeguarding or behaviour concern as appropriate;
- review AI-related risks as part of the annual online safety risk assessment and filtering/monitoring review.

Where the school procures or adopts AI-enabled educational technology, leaders will consider the DfE's current generative AI product safety standards and data protection requirements before approval.

7. Cyber security, information security and access management

Cyber security is a safeguarding issue because a cyber attack or data breach can expose children's personal information, safeguarding records or health information and disrupt systems needed to keep children safe.
The school will maintain proportionate technical and organisational measures to protect information and systems, including secure passwords, appropriate access permissions, software updates, backups, anti-malware protections and staff awareness. The school will work towards and maintain the DfE cyber security and wider digital and technology standards as appropriate to its setting.
Access to school systems will be limited to authorised users and appropriate levels of access. Users must not access another person's account, share passwords or deliberately bypass security controls. Suspected phishing, malware, unauthorised access or data loss must be reported immediately through the school's agreed reporting route and, where relevant, to the DSL, Data Protection Officer and IT support/provider.

8. Email, messaging and online communication

Staff and governors must use school-approved accounts and systems for official communication. Staff must not use personal email, personal messaging accounts or unapproved platforms to contact pupils or conduct school business.

Communication with parents/carers and pupils must be professional, appropriate, traceable and consistent with the school's safeguarding and data protection arrangements. Staff must not send, receive or share offensive, discriminatory, humiliating, threatening or otherwise inappropriate communications.
Suspicious emails, attachments, links or messages must not be opened or followed and must be reported using the school's agreed process. Staff should be alert to phishing, impersonation and financial scams.

9. Websites, apps, downloading and online services

Staff must check websites, software, apps and online services before using or recommending them to pupils. Where an online service requires accounts, personal data, photographs, recordings or other pupil information, staff must follow the school's data protection and procurement/approval arrangements before use.

- Use school-approved systems for blogs, wikis, learning platforms and other online communication spaces.
- Use age-appropriate search tools and safe-search settings.
- Do not download or install software or browser extensions without appropriate authorisation.
- Observe copyright and licensing requirements.
- Do not deliberately access, create, upload, download or distribute illegal, abusive, hateful, extremist, violent, pornographic or otherwise harmful material.
- Do not use school systems to intimidate, threaten, harass, discriminate against or cause harm to another person.
- Do not use school hardware or networks for unauthorised commercial activity or to interfere with the normal operation of systems.

10. Images, video and personal data

Photographs and videos can support learning and celebration of pupils' achievements, but they are personal data and may create safeguarding risks. The school will use images in accordance with its data protection/privacy arrangements and recorded consent processes where required.

- Only school-approved equipment and systems may be used by staff to record images of pupils unless an explicit exception has been authorised for a safeguarding, medical or emergency purpose.
- Images and videos must be stored only in approved secure locations with access limited to authorised users.
- Images must not be copied to personal devices, personal cloud storage or personal messaging services.
- Temporary working copies must be transferred to approved storage and deleted promptly where appropriate.
- Staff must consider children whose images must not be shared because of safeguarding, court, consent or other circumstances.
- Parents/carers must follow the school's arrangements for photography and filming at school events and must not publish images of other children without appropriate permission.

Before introducing a new system that processes images, monitoring data or other high-risk personal information, the school will consider whether a Data Protection Impact Assessment is required and will consult the Data Protection Officer as appropriate.

11. Mobile phones and personal devices

The school will maintain a mobile phone environment consistent with the DfE expectation that schools should be mobile-phone-free by default, with exceptions only where a clear need has been identified.
For pupils, personal mobile phones are not permitted in school.
Staff and visitors must not use personal mobile phones or personal devices for personal purposes in the presence of pupils except where specifically authorised for an educational, safeguarding, medical, emergency or other legitimate school purpose.

Staff must not use personal devices to photograph, video, record or directly communicate with pupils unless expressly authorised under a school-approved procedure. School business should be conducted using school-provided or school-approved devices and systems.
Personal devices brought onto the premises must not contain inappropriate or illegal content. The school is not responsible for loss, damage or theft of personal devices, subject to any other applicable school arrangements.

12. New technology, remote learning and off-site provision

New technologies can offer educational benefits but must not be introduced on the assumption that they are safe. The school will consider educational purpose, age appropriateness, safeguarding, data protection, accessibility, filtering/monitoring, cyber security and staff competence before approving new technologies.
When pupils are learning remotely or using digital platforms away from school, the same safeguarding principles apply. The school will use approved platforms, clear staff/pupil expectations, appropriate access controls and parental communication. Staff must report safeguarding concerns arising during remote learning through the usual safeguarding route.
Where pupils receive education off site, attend trips or access provision through another organisation, the school will take reasonable steps to ensure that relevant safeguarding and online safety expectations are understood and that appropriate due diligence is completed.

13. Reporting, responding to and recording incidents

Any pupil or adult who receives an offensive, abusive or inappropriate message, accidentally accesses upsetting or harmful material, or becomes aware of unsafe online activity must report it promptly to the first available member of staff, the DSL/deputy DSL or the Headteacher.
Where an incident may indicate risk of harm, staff must follow the Child Protection and Safeguarding Policy immediately. Staff must not investigate, forward harmful material unnecessarily, or delay reporting while trying to establish what happened.
The school will record online safety incidents using its agreed safeguarding/incident recording system. Records should be factual and proportionate and should include the concern, actions taken, decisions, rationale and outcomes where relevant.
Where appropriate, the school may seek advice from children's social care, the police, the local safeguarding partnership, the National Crime Agency/CEOP or other specialist services. The school will use the current reporting route and guidance relevant to the incident rather than relying on outdated contact arrangements.
Incidents involving staff or other adults will be managed under the school's safeguarding allegations/low-level concerns procedures as appropriate. Online safety incidents may also be dealt with under behaviour, disciplinary, contractual or other relevant procedures.
The school will provide appropriate support to pupils and staff affected by online harm and will use incident learning to inform curriculum, supervision, filtering/monitoring, training and policy review.

14. Curriculum and digital literacy

Online safety education will be developmentally appropriate and embedded within the curriculum. It will help pupils understand how to recognise risk, seek help, behave respectfully and make safer decisions online.
For children in EYFS and KS1, teaching will include, as appropriate:

- recognising when something online makes them worried, uncomfortable or unsafe;
- knowing trusted adults they can talk to;
- understanding that not everyone online is who they say they are;
- understanding that some content is not suitable for children;
- using devices and apps safely and responsibly;

- protecting personal information and understanding privacy;
- seeking help when something goes wrong;
- treating others respectfully online and understanding cyberbullying;
- understanding that photographs, videos and messages should not be shared without appropriate permission;
- recognising advertising, commercial content, scams and persuasive design at an age-appropriate level;
- understanding that technology and AI can create content that is not real or trustworthy;
- developing critical thinking and media literacy so pupils can question misleading, manipulated or false information.

Curriculum content will be responsive to emerging risks and relevant incidents affecting the school community. Where an online issue is identified, the school may adapt teaching, assemblies, parent communication or pastoral support accordingly.

15. Staff, governor and volunteer training

All staff and governors will receive appropriate online safety and safeguarding training. Training needs will be reviewed regularly and recorded as part of safeguarding records.

Training will cover, as relevant to role: online harms; reporting routes; filtering and monitoring; safe use of school systems; data protection; cyber security; AI; mobile phone expectations; emerging threats; and the needs of pupils who may be particularly vulnerable online.

New staff will receive this policy and the relevant Acceptable Use Agreement as part of induction. Supply staff, student teachers, peripatetic staff, regular visitors, volunteers and contractors will receive appropriate information and instructions before or when they begin working with pupils.

16. Working with parents and carers

The school will work with parents and carers to help children use technology safely and responsibly at home and at school. Communication will include practical advice about online harms, age-appropriate use, parental controls, reporting concerns, healthy digital habits, scams, privacy and emerging risks such as AI-generated content.

Parents/carers will be informed about the school's filtering and monitoring arrangements at an appropriate level, including the purpose of monitoring and how online safety concerns are handled. The school will also explain expectations for children using school platforms or communicating with staff online.

Acceptable Use Agreements and other relevant expectations will be communicated to families in line with the school's current arrangements.

17. Monitoring, review and assurance

The school will monitor the effectiveness of this policy through safeguarding records, incident trends, curriculum review, staff training, pupil and parent feedback where appropriate, filtering and monitoring checks, cyber security reviews and governor oversight.

The policy will be reviewed at least annually and sooner where there are significant changes to legislation, statutory guidance, technology, school systems, online risks or lessons arising from incidents. The annual review will consider the effectiveness of filtering and monitoring and the school's annual online safety risk assessment.

The governing body will receive sufficient information to understand significant online safety risks, incidents, actions and assurance. Records of annual filtering and monitoring checks will be retained and made available to relevant leaders and inspectors where appropriate.

This policy supports the school's safeguarding arrangements and the evidence inspectors may consider under the current Ofsted inspection framework, including leaders' and governors' whole-school approach to safeguarding, pupils being taught how to stay safe online, and the effectiveness of information systems in safeguarding pupils from online harm.

Appendix 1 – Online safety incident record

Complete this record in line with the school's safeguarding and data protection procedures. Do not attach harmful or illegal material to this form. Preserve evidence safely and seek advice from the DSL/police/appropriate agency where necessary.

Field	Record
Name of person reporting incident	
Date/time reported	
Date/time of incident	
Location/device/platform	
Inside school / outside school / remote learning	
Who was involved?	Pupil(s), staff, parent/carer, visitor, other
Description of concern	
Online risk area	Content / Contact / Conduct / Commerce
Type of incident	Cyberbullying; grooming/exploitation; inappropriate content; sexualised images; AI/deepfake; account/security; phishing/scam; hate/extremism; other
Evidence available and where stored	Do not attach harmful/illegal material to this form
Immediate action taken	
Reported to DSL/deputy DSL	
Safeguarding advice/referral	
Police/CEOP/other agency contact	
Parent/carer informed	
Support offered to child/staff	
Filtering/monitoring action required	
Policy/curriculum/training action required	
Outcome and follow-up	

Appendix 2 – Annual filtering and monitoring assurance record

Complete at least once each academic year and retain with safeguarding/governance records. This record is designed to evidence the school's annual check of filtering and monitoring effectiveness across relevant internet-connected devices and locations.

Assurance item	Evidence / finding / action
Date of annual review and check	
Person responsible (SLT) and DSL involved	
Filtering provider/system confirmed and current	
Monitoring provider/system confirmed and current	
All relevant school-managed devices checked	
All relevant locations/networks checked	
Safe-search and age-appropriate settings checked	
User identification/traceability confirmed	
Monitoring alerts/reports reviewed and escalation route tested	
Temporary exceptions reviewed and authorised	
AI-related risks and AI-enabled tools considered	
Pupil vulnerabilities/age profile considered	
Privacy notice/data protection arrangements checked	
Cyber security dependencies/risks considered	
Incidents and lessons learned considered	
Actions identified, owners assigned and deadlines recorded	
Actions completed/monitored	
Governors/School Development Committee assurance provided	
Next review/check date	