Online Safety Policy

CUFFLEY
A Foundation School

Ratified:	**November 2026**
Chair of Governors:	**Marie Linnane**
Review:	**November 2027**

Contents

1. Introduction & Statutory Framework

2. Roles and Responsibilities & Key Safeguarding Personnel Table

3. Scope of Policy & Interlinked Policies

4. Acceptable Use, Prohibited Content, Device Security & Cloud Infrastructure

5. Image Storage, Personal Mobile Devices & Mobile Phone-Free Environment

6. Artificial Intelligence (AI) Policy: Safe Staff Research, Planning & Data Protection

7. Filtering, Monitoring Standards & Cyber Security Standards

8. Incident Logging, CPOMS, Senso & Operation Encompass Duties

9. Online Safety Curriculum, RSHE & Preventative Education

10. Staff Training, Safer Recruitment & Teacher Status Checks

11. Working in Partnership with Parents/Carers

12. Policy Monitoring, Incident Logging & Review

Appendices of the Online Safety Policy (Appendices A – K)

1. Introduction and statutory framework

Cuffley School recognises that internet, mobile and digital technologies provide valuable opportunities for children and young people to learn, socialise, and play, but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules or ones that are constantly evolving. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff, and governors will be equipped to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently. This policy reflects the statutory duties set out in Keeping Children Safe in Education (KCSIE) 2026, Working Together to Safeguard Children, the Online Safety Act 2023, the Data Protection Act 2018, the UK GDPR, the Data (Use and Access) Act 2025, and the Crime and Policing Act 2026. While the Online Safety Act primarily regulates online platforms, Cuffley School actively enforces its principles by educating pupils on age-appropriate access, digital resilience, and reporting mechanisms. While the Online Safety Act primarily regulates tech companies, schools have a duty to educate and safeguard pupils in line with its principles.

2. Roles and Responsibilities

The headteacher, Wendy Wing, and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named Online Safety Lead in this school is Rachel Evans. All breaches of this policy must be reported to Rachel Evans and/or Wendy Wing.

All breaches of this policy that may have put a child at risk must also be reported to the Designated Safeguarding Lead, Tracy Farmer or Deputy Designated Safeguarding Leads – Wendy Wing and Rachel Evans.

DSL Availability and Cover Arrangements

In accordance with KCSIE 2026 requirements, Cuffley School ensures continuous safeguarding cover during term time and out of hours activities. A DSL is always available and the admin@cuffley.herts.sch.uk email is monitored.

Post	Post holder
Headteacher	Wendy Wing
Online Safety leader	Rachel Evans
Safeguarding Governor	Leanne Raffety
Safeguarding leader (DSL)	Tracy Farnmer
Deputy Safeguarding leaders (DDSLs)	Wendy Wing Rachel Evans Andrea Charalambous Charlie Lloyd
Date Protection Officer (DPO)	Nadine Grainger

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy and interlinked Policies

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors and volunteers
- voluntary, statutory or community organisations using the school's facilities.

The school also collaborates with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, Health and Safety, home–school agreement, home learning through the Google Classroom, Behaviour, Anti-bullying and Personal Social Health Education/Relationships and Sex Education policies.

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

4. Acceptable Use, Prohibited Content, Device Security and Cloud Infrastructure

4.1 Use of email and official communication

Staff and governors must use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Children at Cuffley School all have Google Classroom logins from Nursery where parents can receive information from the school and support their pupils learning. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission, refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Rachel Evans or Wendy Wing

Users must not send emails which are offensive, embarrassing, or upsetting to anyone (i.e. cyberbullying).

4.2 Visiting online sites, Search Engines and downloading.

Staff must preview sites, software, and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer (DPO), Nadine

Grainger, with details of the site/service and seek approval from Rachel Evans or Wendy Wing. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content that supports our computing Curriculum – Teach Computing a DFE recommended programme of work.

- When working with pupils searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine. Staff are aware or safe internet search sites for pupils, these include: Kiddle, KidzSearch, Kidrex, Kid Topia, Sweet Search, Fact Monster and Google Scholar.

4.3 Prohibited Behaviours and the Four Cs of Online risk (KSCIE 2026 Alignment)

In line with KCSIE 2026, and the categorisation of the four distinct areas of harm (4Cs- Content, Contact, Conduct, Commerce) users at Cuffley must not visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- **Content (Harmful & Illegal Material):**
- **Child & Vulnerable Person Abuse Imagery:** Indecent images of children actually or apparently under the age of 18 or child abuse material (including photographs, videos, digital images, cartoons, or AI-generated imagery depicting children involved in sexual activity or posed sexually provocatively), as well as indecent images of vulnerable adults over 18.
- **Adult & Obscene Material:** Adult explicit material that breaches the UK Obscene Publications Act, extreme pornography, or extreme physical violence.
- **Discrimination & Hatred:** Material promoting discrimination, prejudice, or hatred of any kind in relation to protected characteristics under the Equality Act 2010 (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation), including misogyny, misandry, racism, and antisemitism.
- **Illegal Acts & Radicalisation:** Material promoting illegal acts (including physical or sexual abuse of children or adults, violence, bomb-making, drug/alcohol abuse, software piracy, or cybercrime), radicalisation, extremism, fake news, disinformation, or conspiracy theories.
- **Reputational Harm & Disrepute:** Any material that may bring Cuffley School or any individual within it into disrepute, including the promotion of violence, gambling, libel, defamation, or disrespect.
- **Contact (Harmful Online Interactions):** Peer-to-peer pressure, commercial advertising, adults posing as children/young adults to groom or exploit for sexual, criminal, or financial purposes, or harmful interactions with Generative AI applications simulating human contact.
- **Conduct (Harmful Online Behaviours):** Making, sending, or receiving non-consensual explicit images (including AI-generated nudes, semi-nudes, deepfakes, or deep nudes), cyberbullying, misogynistic/misandrist messaging, targeted harassment, upskirting, or non-consensual image sharing.
- **Commerce (Commercial & Financial Risks):** Online gambling, age-inappropriate advertising, phishing, or financial scams. (Phishing or financial fraud attempts must be reported to the Anti-Phishing Working Group at apwg.org).

4.4 User Conduct & System Security Restrictions

To maintain system integrity, personal safety, and statutory data security, users must **NOT**:

- **Confidentiality:** Reveal, share, or publicise confidential, personal, or proprietary school information without authorisation.
- **System Integrity:** Intentionally interfere with the normal operation of the school's internet connection or IT infrastructure, including the propagation of computer viruses, malware, or ransomware.
- **Unsolicited Spam:** Transmit unsolicited commercial or advertising material to other users or external organisations without explicit prior school permission.
- **Commercial Misuse:** Use the school's hardware, Wi-Fi facilities, or cloud accounts for running a

private business or personal financial gain.
- **Harassment & Intimidation:** Intimidate, threaten, cyberbully, or cause physical, emotional, or reputational harm to others.
- **Account Security:** Access, attempt to access, or interfere in any way with other users' accounts, passwords, or personal files.
- **Prohibited Technology:** Install or use software or hardware that has been prohibited or unapproved by the school leadership or IT support team.

4.5 Device Security, Remote Working & Cloud Infrastructure Assurance

Staff are strongly advised to conduct all school business outside of school using a school-owned device. Conducting school business on personal devices is restricted; the only permitted exception is where the school has configured a closed, monitorable system. Such a system ensures that users cannot save files locally to their personal device, thereby preventing personal data breaches under the Data Protection Act 2018 / UK GDPR

As a school, we work through a cloud-based systems that is hosted and managed online, rather than locally in the school buililding. Working in -based services makes it easier to access applications and content, wherever there is an internet connection. This system has reduced the workload of the local technical support team (HFL), as applications can now be automatically updated and managed mitigating the risk of files and data being lost. It could also support flexible working as you can access data remotely at any time. This system gives staff the flexibility to access services from wherever they are, using the devices that are most convenient for them. However, we do recommend a school device. Furthermore, collaboration within documents helps staff to easily share and co-author documents, files, lesson content and plans, thus reducing duplication of effort.

Cloud services can have native security advantages over local or on premises technology. While organisations can have less visibility of the underlying infrastructure and operations, cloud providers can use economies of scale to provide a level of security that would be economically or operationally infeasible for many organisations. As HFL are our technology support and advisors we are confident that the systems provided by them are secure.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police where appropriate.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use, e.g. for staff development, staff meetings and training. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Wendy Wing or Rachel Evans.

5. Image Storage, Personal Mobile Devices and mobile Phones

Storage and use of images/videos

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file, and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by Wendy Wing. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals collaborating with pupils, must only use school equipment to record images of pupils whether on or off site unless specifically agreed with Wendy Wing. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is in the personnel file.

Use of Personal Mobile devices

In strict compliance with DfE statutory guidance on Mobile Phones in Schools and KCSIE 2026, Cuffley School is a mobile phone-free environment by default for all pupils throughout the entire school day. This applies during lessons, breaktimes, lunchtimes, and transit between classes. Pupils are prohibited from bringing personal mobile devices or phones to school. Any exception is strictly by prior written agreement with Headteacher Wendy Wing for specific medical or safeguarding reasons.

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Only under exceptional circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device. If this is necessary, the staff member must block their number beforehand.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child unless there is a pre-specified permission from Wendy Wing. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

6. Artificial Intelligence (AI)

In accordance with the HFL Education AI Policy Guidelines (v1.2, January 2026), DfE guidance on 'Generative Artificial Intelligence in Education', and DfE 'Generative AI: Product Safety Expectations', Cuffley School recognises that Artificial Intelligence (AI) offers valuable opportunities to support educational research, lesson planning and administrative efficiency. However, Cuffley School explicitly DOES NOT permit pupils to use or interact directly with Generative AI tools or platforms. Standard terms and conditions for commercial Generative AI platforms state that users must be at least 13 years old (or older). As a primary school setting, children do not possess personal accounts for, nor are they permitted to directly operate, Generative AI applications. Pupil interaction with AI is strictly restricted to learning about AI concepts, age restrictions, digital literacy, and safety within the taught Computing and PSHE curriculum (e.g. Year 6 'The Big AI Project').

Leadership, teaching, and support staff are permitted to use approved AI tools safely, ethically, and responsibly to assist with professional duties.

AI Governance and Approved Systems

- All Artificial Intelligence tools used for school purposes must be approved by the Headteacher, Online Safety Lead and Data Protection Officer prior to use.
- The school will maintain an Approved AI Register which documents all authorised AI tools, approved use cases, associated risk assessments, DPIAs and review dates.
- Staff must not use unapproved AI applications, browser extensions, websites, chatbots, or AI-powered educational platforms for any school-related activity.
- Any proposed AI tool must undergo a safeguarding review, cyber security review and, where appropriate, a Data Protection Impact Assessment (DPIA) before approval is granted. Department for Education guidance recommends schools consider safeguarding, privacy, security, and intellectual property implications before adopting AI products.

Permitted professional use cases include:

- Conducting background educational research and gathering curriculum ideas.
- Assisting with lesson planning, scheme of work structuring, and drafting classroom materials.

- Adapting reading texts or curriculum content to different reading levels to support differentiation.
- Generating administrative templates, exemplar prompts, and creative educational ideas.
- Staff must ensure that all use of AI complies with data protection legislation and school data protection policies. The following non-negotiable rules apply to all staff:
- Staff must NEVER input, upload, paste, or process any personal data relating to pupils, staff, governors, or parents into any AI tool. This includes names, dates of birth, addresses, photos, medical/SEND info, assessment figures, or CPOMS safeguarding notes.
- Staff must not upload pupil work, assessment information, behaviour records, attendance information, SEND records, medical information, safeguarding information, CPOMS records, staff records or parent information to any AI platform unless specifically authorised following completion of a DPIA.
- Staff must not enter information into AI systems that could directly or indirectly identify a child, family member, or member of staff.

Staff remain individually responsible for ensuring compliance with the UK GDPR, Data Protection Act 2018 and school data protection procedures when using AI systems.

Any suspected AI-related data breach must be reported immediately to the DPO and Headteacher and managed in accordance with the school's data breach procedures. Department for Education guidance highlights the importance of data privacy and intellectual property when using generative AI.

- Pupil work, writing, or creative submissions must NEVER be uploaded into AI tools for marking, feedback, or processing. This protects pupil privacy and ensures pupil intellectual property is never used by external commercial platforms to train AI models.
- Any AI software or tool that processes data or integrates with school systems must undergo a formal DPIA overseen and approved by Data Protection Officer Nadine Grainger prior to deployment.

AI applications are prone to generating inaccurate information ('hallucinations'), bias, or outdated content. Staff maintain sole human responsibility for all curriculum content and administrative outputs:

- All AI-generated content (lesson plans, adapted texts, worksheets) MUST be critically reviewed, fact-checked, and edited by a staff member before being used in the classroom.
- Staff must exercise professional judgement to ensure outputs are accurate, unbiased, age-appropriate, and aligned with school values.

To ensure due diligence and safety, staff are restricted to using the following pre-vetted tools strictly within approved parameters:

- Google Gemini: Conversational AI accessible through school Google for Education accounts. Approved for generating lesson plans, adapting text reading levels, and drafting materials. Strictly NO personal data or pupil work.

Approved AI Tools

- Google Gemini (Education)
- Microsoft Copilot (Education)
- Google Gemini Notebook (Education Accounts only)
- Any additional systems formally approved by the Headteacher, Online Safety Lead and DPO

Use of any AI platform not included within the school's Approved AI Register requires written approval before use.

All staff will annually declare which AI tools they access or use in connection with school business.

The Online Safety Lead and Data Protection Officer will conduct an annual review and survey of AI use across the school. Outcomes from the annual review will inform staff training, safeguarding risk assessments, cyber security review processes, and policy development.

7. Filtering and Monitoring and Cyber Security

Cuffley School employs a dual layer of protection: Senso Safeguarding Monitoring (monitoring

keystrokes, typed vocabulary and active across Windows devices and Chrome books and Rm SafetyNet (HFL Education broadband filtering blocking inappropriate or illegal web content).

In strict compliance with KCSIE 2026 filtering and monitoring standards, an annual review of the effectiveness of filtering and monitoring systems is conducted jointly by the SLT member responsible for filtering, Rachel Evans, and IT support (HFL Education). This includes physical checks that filtering is working appropriately on all internet-connected devices in all locations across the school, with written records maintained.

The school self- assesses with 360 Safe to ensure complete compliance and uses DFE 'Plan Technology' for your school as a reference for compliance.

Filtering and monitoring reviews will specifically evaluate risks associated with Generative AI, AI generated content, AI chatbots, deepfakes, nidification tools and AI-assisted searching.

Annual filtering and monitoring reviews will include consideration of which AI platforms are blocked, allowed, or monitored within the school environment.

AI-generated content presents safeguarding risks that must be considered as part of annual filtering and monitoring reviews.

All approved AI products will be evaluated against Department for Education Generative AI Product Safety Expectations prior to implementation.

In line with DfE Cyber Security Standards for Schools and Colleges and NCSC guidance, Cuffley School implements robust technical safeguards including secure password policies, role-based access controls, regular data backups, network firewalls, and staff anti-phishing awareness. We use Cheeky Monkey Security to train staff and keep Cyber Security training up to date and at the forefront of thought.

8. Incident Logging and reporting

All breaches or online safety concerns must be reported immediately to Rachel Evans or Wendy Wing and logged. Senso Automated alerts are reviewed daily and Safety Net weekly at varying intervals.

Incidence involving any sharing of nudes/semi-nudes (consensual or non- consensual) trigger an immediate safeguarding response. Staff know not to view or forward explicit images and parents as well as staff are sign posted to ChildLine/IWF 'Report and Remove 'tool.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

AI-related safeguarding concerns, including deepfakes, manipulated imagery, impersonation, nidification applications and AI-assisted bullying will be recorded on CPOMS and managed in accordance with safeguarding procedures.

9. Online Safety Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe, and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education. As a school we follow the Jigsaw scheme

of work and Teach computing for our computing lessons both of which have online safety embedded within them.

Our curriculum is informed by the **UK Council for Internet Safety (UKCIS) framework "Education for a Connected World"** and supported by resources such as **ProjectEVOLVE**, ensuring progression in digital resilience and online safety from EYFS to Year 6.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience, and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic, and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity. Year 6 children develop their digital leadership skills by participating in a Digital Leadership programme. With parental consent, they develop the skills and knowledge to educate and train their younger peers on how to use technology safely and effectively.

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment.

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

    - Understanding the permanency of all online postings and conversations

    - Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation, and images.

    - Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

    - How the law can help protect against online risks and abuse.

    - Children are now living in a world of Artificial Intelligence (AI). We are developing our curriculum to support their understanding and use of AI. As part of this curriculum, we will be working with The Big AI project and will deliver lessons in Year 6. As the project develops, we intend to disseminate the lessons, where appropriate, throughout the school. Children will, in computing lessons, also discuss scenarios about AI as part of their safeguarding learning. As AI becomes more integrated into education, the school ensures that any AI tools used by staff or pupils are risk assessed, age-appropriate, and monitored. Staff are trained to identify misuse or over-reliance on AI, and pupils are taught to critically evaluate AI-generated content.

10. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. We have a designated teacher Governor and Designated Safeguarding Lead (DSL), Tracy Farmer, who works with the DSL team and the online safety and computing curricular leaders as and when necessary

to keep updated with training needs and procedures within the school. Leanne Rafferty is our nominated Safeguarding Governor.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B). Personalise as required.

Peripatetic staff, student teachers, and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B

Guidance is provided for occasional visitors, volunteers, and parent/carer helpers (Appendix E).

11. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of modern technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked to read, discuss, and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

12. Appendices of the Online Safety Policy

A. Online Safety Acceptable Use Agreement - Staff, Governors, and student teachers (on placement or on staff) Responses will be on a Google Document
B. Online Safety Acceptable Use Agreement – Herts Music Service and holiday clubs
C. Online safety agreement – Peripatetic teachers/coaches and supply teachers
D. Requirements for visitors, volunteers and parent/carer helpers working in the school (working directly with children or otherwise)

E. Online Safety Acceptable Use Agreement Primary Pupils - discussed with pupils and

   posted o the Computing Google classrooms.

F. Online safety policy guide - Summary of key parent/carer responsibilities

G. Guidance on the process for responding to cyberbullying incidents.

H. Guidance for staff on preventing and responding to negative comments on social media.

Appendix A - Online Safety Acceptable Use Agreement
Staff, Governors, and student teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement, and it will be kept on record in the school. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Rachel Evans or Wendy Wing. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Rachel Evans or Wendy Wing.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers, or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely.

- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body.

- Personal or sensitive data taken off site must be encrypted.

Images and videos

I will only upload images or videos of staff, pupils, or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device unless given permission by Wendy Wing e.g. on school trips. Images taken should be promptly deleted once transferred to the Staff Drive or Google Classroom.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Rachel Evans or Wendy Wing.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will always promote positive online safety messages including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils, or parents/carers) to the DSLs or Headteacher.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with a member of SLT.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Responses and a declaration of acceptance are via a Google form.

Appendix B - Online Safety Acceptable Use Agreement

Peripatetic teachers/coaches, supply teachers

CUFFLEY SCHOOL

Online safety Lead: Rachel Evans

Designated Safeguarding Lead (DSL): Tracy Farmer
Deputy DSLs: Wendy Wing and Rachel Evans

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record, and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Rachel Evans. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Rachel Evans.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with Wendy Wing

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over thirteen and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on

personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers, or pupils. Privileged information known because of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs, and videos. Once agreed, these must be made on a school device.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils, or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupils or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions, but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the headteacher/DSL, or a young person's or parent/carer's own device.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Rachel Evans.

Promoting online safety

I understand that online safety is part of my responsibility and I will always promote positive online safety messages, including when setting homework, rehearsal, or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSLs or SLT members.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Wendy Wing.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership and DSLs. A school-owned device should be used when running videoconferences, where possible.

Data protection

Artificial Intelligence, Approved Websites and Approved Online Services

I understand that: I may only use websites, applications, software, and Artificial Intelligence platforms approved by Cuffley School.

I must seek permission from Rachel Evans, Wendy Wing, and/or the Data Protection Officer before using any online platform, application or AI tool that has not been previously approved by the school.

I must not create pupil accounts on websites, applications or AI systems that have not been approved by the school.

I must not enter pupil data, safeguarding information, SEND information, behaviour information, medical information, assessment information, or any personally identifiable information into any AI platform.

I understand that AI-generated outputs may contain inaccurate, incomplete, biased, or misleading information and that I remain professionally responsible for checking and verifying all outputs before use.

I will immediately report concerns involving AI-generated content, deepfakes, manipulated images, impersonation, cyberbullying, or misuse of AI systems to the DSL.

I understand that all AI use must comply with UK GDPR, the Data Protection Act 2018 and the school's safeguarding procedures.

I understand that my use of AI systems may be reviewed as part of the school's annual AI audit and online safety monitoring arrangements.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Agreements and acceptance declarations are via a Google Form which is emailed to all staff on a yearly basis and a central record kept by Tracy Farmer (DSL)

Appendix C - Requirements for visitors, volunteers, and parent/carer helpers

(Working directly with children or otherwise)

School name: Cuffley School

Online safety lead: Rachel Evans
DSLs: Wendy Wing, Tracy Farmer, and Rachel Evans

Safeguarding rules for visitors and volunteers: raise safeguarding concerns immediately with Wendy Wing or Tracy Farmer, switch off personal mobile devices outside designated areas, never take photographs on personal devices, and maintain strict confidentiality.

Volunteer DBS Notice (Crime & Policing Act 2026): Volunteers supervising or working with children frequently (>3 days in 30 days) or overnight must undergo an enhanced DBS check with children's barred list check prior to commencing duties.

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSLs

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSLs are informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems, and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content, I plan to use I will check with my contact in the school.

Appendix D - Online Safety Acceptable Use Agreement Primary Pupils (posted on Computing Google classrooms and discussed with pupils)

My online safety rules

Pupil Online Safety Rules (discussed in class and posted on Computing Google Classrooms):

1. I will only use school IT equipment for activities agreed by school staff.
2. I will not use my personal email address or personal accounts in school.
3. I will keep my passwords private and never use someone else's username or password.
4. I will make sure all online contact is polite, responsible, kind, and respectful always.
5. If I come across anything upsetting, nasty, or unsafe, I will tell my teacher or parent immediately.
6. I will not give out personal details (full name, phone number, address, school) online.
7. I will never upload images or videos without permission from my teacher and parents.
8. I will never arrange to meet someone I only know online.
9. I will follow the mobile phone-free school rules and never bring personal devices into school unless agreed.
10. I understand that creating or sharing hurtful content, rumours, or nude/semi-nude images (including AI deepfakes) is unacceptable and illegal

Dear Parent/Carer,

The internet, email, mobile technologies, and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with Wendy Wing or a member of the Senior Leadership Team.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

Pupil name……

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature…….

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils, and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren unless there

is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)…….

Parent/carer signature…….

Date ……..…..…

Appendix E - Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, consulting with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group, or any other online presence that uses the school's name or logo in any form.

- Any parent/carer distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils, and parents/carers.

Appendix F - Guidance on the process for responding to cyberbullying incidents.

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community most cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecently images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will investigate.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary, the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking are also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.
- Cases involving sexual harassment, upskirting, non- consensual image sharing, or AI deepfakes will be referred to the police or social care.

Appendix G - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts.

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

  The meeting must:

  - Draw attention to the seriousness and impact of the actions/postings.
  - Ask for the offending remarks to be removed.
  - Explore the complainant's grievance.
  - Agree next steps.
  - Clarify the correct complaints procedures.

  If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

  - Reporting the matter to the social network site if it breaches their rules or breaks the law.
  - Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking are also a crime.

  If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix K – Safeguarding and remote education

Useful resources

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

- **DfE Safeguarding and Remote Education**
https://www.gov.uk/guidance/safeguarding-and-remote-education

- **The Key for School Leaders: Remote Learning, Safeguarding Pupils and Staff**
https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body

- **NSPCC: Undertaking Remote Teaching Safely**
https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely

- **LGfL: Twenty Safeguarding Considerations for Lesson Livestreaming**
https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

- **SWGfL: Remote Working, A Guide for Professionals**
https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf

- **National Cyber Security Centre: Video Conferencing, Using Services Securely**
https://www.ncsc.gov.uk/files/vtc_infographic.pdf

- **DfE: Teaching About Relationships, Sex and Health (RSHE Hub)**
https://www.gov.uk/guidance/teaching-about-relationships-sex-and-health

- **UK Safer Internet Centre: Appropriate Filtering and Monitoring**
https://www.saferinternet.org.uk/

- **Childline / IWF Report Remove Tool**
https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online/