Cavendish Close Infant and Nursery School
Online-Safety Policy

What's different about this policy for September?

This year, changes have been made to reflect trends seen over the past year. There is some added content about the use of CCTV, filming in and outside school, use of generative AI and filtering and monitoring.

Policy review dates and changes

Review date	By whom	Summary of changes made	Date implemented
January 2026	C Brown	Changes made throughout. Updated information regarding online risks this academic year based on evidence collated in 2025. Updated roles and responsibilities for parents and carers. Updated Education and Curriculum information. CCTV section added. Updated Bullying section. Information added on responding to issues that arise from 'banter'. Updated information with regards to appropriate filtering and monitoring. Updated information on our use of generative AI. RAG rating removed from our school website section. Updated information in 'Digital images and video' section regarding not sharing photos without permission. Addition information added to CCIS Social Media presence. Information regarding conducting regular checks of privacy and security settings on social media accounts added. Addition information added under 'Device Usage' for parents, regarding Apple AirTags. Updated information on trips and events away from school.	
January 2025	C Brown	Changes made throughout. AUPs to be updated annually for all stakeholders. Updated information regarding online risks this academic year based on evidence collated in 2024. Updated information in relation to how this policy will be communicated. AUPs are to be displayed and accessible in school. 'Further help and support' section removed. Updated scope. Updated roles and responsibilities in relation to filtering and monitoring: All staff, DSL/OSL and Network Technician. Updated Education and Curriculum section. Information added on how fundamental technology is for adult life and how parents/carers are informed of online safety learning. Updated information on handling online safety concerns and incidents. 'Actions where there are concerns about a child' section removed. Sub-sections: Nudes, Upskirting, Bullying and Child-on-child sexual violence and sexual harassment updated. Extremism section added. Updated information on data protection and cybersecurity. Additional information on regular filtering and monitoring checks to inform practice. Use of generative AI section added. Updated information on online storage or learning platform. Additional information regarding copyright added to the school website section. Additional information added to Staff, pupils and parents SM presence, focusing on the importance of consent before using photographs, videos or personal information.	
November 2023	C Brown	Significant changes made throughout. Strong focus on filtering and monitoring in line with KCSIE.	

		Strong emphasis on implementing AUPs throughout. Updated key people – Deputy DSLs, link governor for online safety and school business manager added. Updated information regarding online risks this academic year based on evidence collated in 2023. Updated information in relation to how this policy will be communicated. Updated roles and responsibilities with focus on filtering and monitoring: Headteacher, DSL/OSL, Governing Body (link Governor responsibilities), All Staff (condensed to one section), Personal Development and RHE lead, Network Technician, DPO, Pupils and Parents/Carers. Additional information added with regards to parents and carers understanding current filtering and monitoring in place in school. Increased reference to school's data protection and cybersecurity policies. Terminology of 'Sexual violence and harassment' has been replaced with 'Child-on-child sexual violence and sexual harassment'. Terminology for 'data security' has been replaced with 'cybersecurity'. Electronic communications section replaced with Messaging/ commenting systems, with 3 subsections – Authorised systems, Behaviour Usage principles and Online storage or learning platforms. School website information updated. Cloud platforms section removed. Additional information added regarding social media age ratings and the importance of sharing these with the school community. Network/Internet access on school devices replaced with 'Use of school devices'. Appendices condensed to reflect key documentation in policy.	
September 2022	C Brown	Changes made throughout Increased focus on a whole school approach when addressing online safety. Update of 4Cs: Commerce is now in place of Contract. Additional information in relation to safeguarding and leadership teams understanding filtering and monitoring. Updated roles and responsibilities: Headteacher, DSL/OSL, All Staff, Personal Development/ RHE lead, Network technician. Additional information in relation to school seeking support from other agencies where necessary. Updated information in relation to sexual violence and harassment. Updated information in relation to staff and parents social media presence.	

Cavendish Close Infant and Nursery School Online-Safety Policy

Contents

Introduction

Key people / dates

Cavendish Close Infant and Nursery School	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring.	Mrs C Diffin Headteacher
	Deputy Designated Safeguarding Leads	Mrs C Howett Deputy Headteacher Mrs N Asghar Assistant Headteacher
	Link governor for safeguarding	Mrs C Moore
	Link governor for Online Safety, including filtering and monitoring.	Mr P Wright
	Online-safety lead	Miss C Brown (Computing lead)
	RHE lead	Mrs A Orme
	School Business Manager, with lead responsibility for communicating with LEAD IT.	Mrs N Tusa
	Date this policy was reviewed and by whom	January 2026 Miss C Brown
	Date of next review and by whom	January 2027 Miss C Brown

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools', statutory RHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school's statutory Child

Protection and Safeguarding Policy. Any issues and concerns with online safety **must** follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we have involved staff, governors, pupils, and parents in writing and reviewing the policy. This helps ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies (AUPs) for different stakeholders will support with this and these should be reviewed annually alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks for this academic year?

Current Online Safeguarding Trends

In our school over the past year, we have noticed an increase in the number of children accessing a digital device daily. Through discussions we identified our children predominantly use technology for playing games and watching videos outside of school.

Nationally, some of the latest trends of the past twelve months are outlined below. These are reflected in this policy and the acceptable use agreements we use and seen in the context of the 5 C's (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding, and technical teams.

Last year, we highlighted the rapid rise of generative AI (GenAI). Since then, the trend has exploded. Thousands of sites now offer AI-generated content, including disturbing levels of abusive, pornographic, and even illegal material like child sexual abuse content. Some platforms host AI "girlfriends," unregulated therapy bots, and even chatbots that encourage self-harm or suicide - tools many children can access freely at home or school. Chatbots can blur reality, offer harmful advice or engage in sexualised and bullying conversations. Their addictive design and unmoderated nature heighten the risk of overuse and exploitation.

When used for generating text, GenAI presents multiple risks. It can spread misinformation, facilitate plagiarism, and most worryingly, bypass safety settings. Many tools lack effective age controls and produce inappropriate content.

Beyond text, GenAI makes it easier than ever to create sexualised images and deepfake videos. These can have a devastating emotional and physical impact on young people, including blackmail and abuse. The Internet Watch Foundation has warned of a sharp rise in AI-generated child sexual abuse imagery. Alarming reports also show children using nudifying apps to create illegal content of peers.

We regularly see AI searches involving sexualised and harmful content. It is critical to stress that in the UK, any CSAM (child sexual abuse material) - AI-generated, photographic, or even cartoon - is illegal to create, possess or share.

Schools must address this not just in the classroom, but by educating parents and students on safe use at home. For guidance and resources, visit genai.lgfl.net.

Ofcom's 'Children and parents: media use and attitudes report 2025' has shown that YouTube remains the most used site or app among all under 18s, followed by WhatsApp, TikTok, Snapchat and Instagram. With children aged 8 - 14 spending an average of 2 hours 59 minutes per day online – with girls spending more time online than boys, four in ten parents continue to report finding it hard to control their child's screentime. Notably, 52% of 8-11s feel that their parents' screentime is also too high, underlining the importance of modelling good behaviour.

Given the 13+ minimum age requirement on most social media platforms, it is notable that over half of 3-12 year olds (55%) were reported using at least one app. Despite age restrictions, four in ten admit to giving a fake age online, exposing them to content inappropriate for their age and increasing their risk of harm, with over a third of parents of all 3-17s saying they would allow their child to have a profile on sites or apps before they had reached the minimum age.

There has also been an increase in online communication platforms that offer anonymous chat services and connect users with random strangers allowing text and video chats. Most of these are easily accessible to children on devices.

As a school we recognise that some of our children may be on these apps regardless of age limits, which are often misunderstood or ignored. We therefore will remind our school community about best practice and respecting age requirements. It is important to remember the reality for most of our children is quite different particularly for those families with older siblings.

This is striking when you consider that 25% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year-olds are being tricked into 'self-generated' sexual content (Internet Watch

Foundation Annual Report) while considered to be safely using devices in the home and for the first time, there were more 7-10 year olds visible in child sexual abuse material (CSAM) images than 11-13s.

Growing numbers of children and young people are using social media and apps, primarily TikTok as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news.

There have also been significant safeguarding concerns where parents have filmed interactions with staff outside the school gates and posted this on social media, putting children and the wider school community at risk of harm.

Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2025 reporting high levels of being attacked nationally, with 60% of secondary schools and 44% of primary schools reporting a breach or attack in the past year.

How will this policy be communicated?

This policy can only impact upon practice if it is a **(regularly updated)** living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website.
- Part of school induction pack for **all** new staff (including temporary, supply and non-classroom based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on **entry** to the school, with annual reminders of where to find them if unchanged and reissued if updated after annual review.
- AUPs will be displayed and accessible in school.

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Cavendish Close Infant and Nursery community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).

- Help safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (in relation to filtering and monitoring) and curriculum leads.
- Help all stakeholders to recognise that online behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - for the benefit of the school, supporting the school vision and ethos, and protecting the reputation of the school and profession.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Behaviour Policy or Anti-Bullying Policy).

Scope

This policy applies to all members of the Cavendish Close Infant and Nursery community (including teaching, supply and support staff, governors, volunteers, contractors, children, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should read the relevant section of this document that describes individual roles and responsibilities. There is one section for **'All Staff'** which **must** be read by everyone, even those who have a named role in another section. All staff have a role to play in feeding back on potential issues.

All Staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, our Safeguarding policy, our code of conduct, and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

All staff must report any concerns, no matter how small, to the designated safeguarding lead as named in the AUP, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond, avoiding scaring and victim-blaming language.

Staff should be aware of the DfE standards for filtering and monitoring and their part in feeding back to the DSL about overblocking, gaps in provision or children bypassing protections. All staff are responsible for the physical monitoring of children's online devices when they are being used in school.

Headteacher – Mrs C Diffin

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the computing team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school).
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnership support and guidance.
- Ensure **ALL** staff undergo safeguarding training (including online safety) at induction and with regular updates. Ensure that they agree and adhere to policies and procedures.
- Ensure **ALL** governors undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements [LGfL's Safeguarding Training for School Governors is free to all governors at safetraining.lgfl.net].
- Understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards. Liaise regularly with LEAD IT to understand what is blocked or allowed for whom, when and how as per KCSIE.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Liaise with the online safety lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.

- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead – Mrs C Diffin / Miss C Brown

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety lead, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring systems** and processes are in place).
- Ensure "An effective whole school approach to online safety as per KCSIE".
- Ensure the school is complying with the DFE's standards on Filtering and Monitoring.
- As part of this, the DSL will work with LEAD IT to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine.
- Where the online-safety leader is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Ensure **ALL** staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
  - This must include filtering and monitoring, to help all staff to understand their roles and responsibilities.
  - All staff must read KCSIE Part 1.
  - Cascade knowledge of risks and opportunities throughout our school.
- Ensure **ALL** governors undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.

- Work closely with the online-safety lead and technical colleagues to complete an online safety audit (including technology in use in school).
- Work with the DPO and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training".
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with Safeguarding, behaviour and Prevent policies) and submit for review to the governors.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net.
- Communicate regularly with SLT, and online safety governor to discuss current issues (anonymised), review incident logs and filtering control logs and discuss how filtering and monitoring work has been functioning.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for families to disclose issues when off site, e.g. emailing the safeguarding team.
- Ensure staff adopt a zero-tolerance, whole-school approach to all forms of child-on-child abuse, and do not dismiss it as banter (including bullying).

Governing Body, led by Online Safety Link Governor and Safeguarding Link Governor – Mr P Wright and Mrs C Moore

Key responsibilities (quotes are taken from Keeping Children Safe in Education):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board.
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.

- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online-safety leader / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.

- Work with the DPO and headteacher to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training (including online safety, with reminders about filtering and monitoring).
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology."

Personal Development and RHE Lead – Mrs A Orme

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the RHE curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives".
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] activities and pupil voice, to capture progress".
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within RHE.
- Ensure the RHE policy is on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Team – Miss C Brown, Mrs K Merriman, Mrs E Wells

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RHE curriculum, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online-safety element.

Network Technician – Lead IT

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.
- Support DSL and OSL to carry out an annual online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE), to support their role as per the DfE standards.

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / RHE lead / data protection officer to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc).
- Ensure filtering and monitoring systems work on new devices and services before releasing them to children and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – Mr John Walker

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the data protection and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records.
- Ensure that all access to safeguarding data is limited as appropriate and is also monitored and audited.

Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safety lead (Mrs C Diffin).
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private or direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, and adhere to the pupil acceptable use policy.

Parents/carers

Key responsibilities:

- Read and adhere to the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it.

External Groups

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Education and curriculum

Despite the risks associated with being online, Cavendish Close Infant and Nursery School recognise the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives

and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

It is important to establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

RHE guidance also recommends schools assess teaching to "identify where pupils need extra support or intervention [through] activities and pupil voice, to capture progress."

The teaching of online safety, features in these particular areas of curriculum delivery:

- Relationships education, and health (also known as RHE)
- Computing

However, as stated in the role descriptors above, it is the role of **all staff** to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind and encourage sensible use, monitor what children are doing and consider potential risks and the age appropriateness of tasks. This includes supporting children with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and conspiracy theories in line with KCSIE 2025), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

At Cavendish Close Infant and Nursery school, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans (including for SEND pupils) take place and are used as an opportunity to follow this more closely in its key areas. This is done within the context of an annual online safety audit, which is a collaborative effort led by Miss C Brown, Online Safety Lead.

We communicate with parents and carers about how we support pupils at our school with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access. These are identified in the Curriculum overviews on the school website.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the DSL with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cybersecurity

This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. The reporting member of staff will ensure that a record is made of the concern on CPOMS.

Any concern or allegation about staff misuse is always referred directly to the Headteacher unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police,

IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

The school will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school will ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

The following sub-sections provide detail on managing particular types of concern.

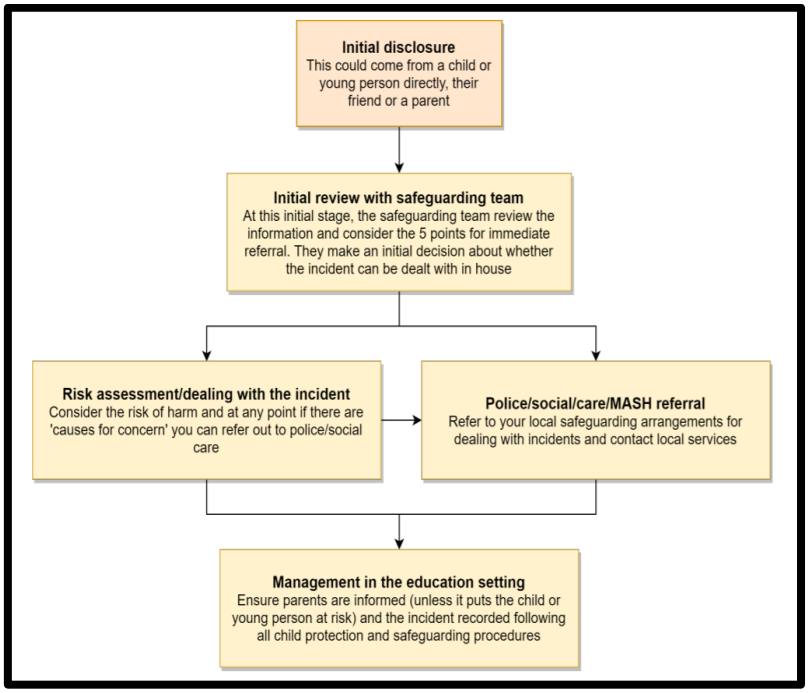
Nudes – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

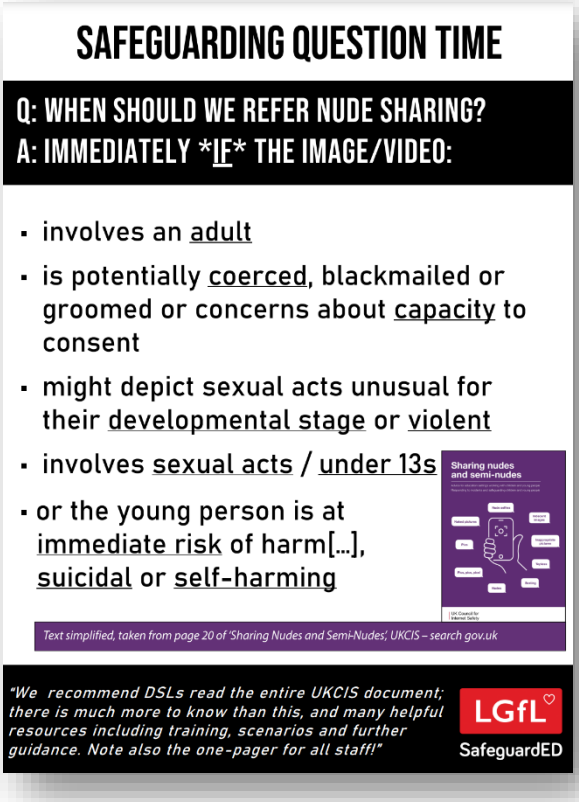
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL**.

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.



The following LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:



Priority Areas

Upskirting

It is important that all staff understand that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse children can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school's Anti-Bullying policy should be followed. This includes issues arising from banter. Our school's Anti-Bullying policy can be found on the school website.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net.

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as the careless use of language. This will be discussed in staff training.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and all staff should follow the safeguarding policy.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults in the Cavendish Close Infant and Nursery School community. These are also governed by schools Acceptable Use Policy.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Cavendish Close Infant and Nursery school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

CCTV

Please find our school CCTV Policy on the school website: https://cavclosei.derby.sch.uk/wp-content/uploads/2025/07/CCTV-policy.pdf.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy which can be found on the school website. It is important to remember that

there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 202, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The designated safeguarding lead (DSL) Mrs C Diffin has lead responsibility for filtering and monitoring and works closely with LEAD IT and Online Safety lead, Miss C Brown, to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure **ALL** staff are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. They can submit concerns at any point to the DSL and will be asked for feedback at the time of an annual review.

Technical and safeguarding colleagues work together closely to carry out annual reviews and checks to ensure that the school responds to issues. LEAD IT carry out half-termly filtering and monitoring checks to ensure all systems are in operation, functioning as expected, and an annual review as part of an online safety audit.

We recognise that generative AI sites can pose data risks, so staff are not allowed to enter any personal information of a member of our school community.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

The DSL checks filtering reports and notifications weekly and takes any necessary action as a result.

According to the DfE standards, "Your monitoring plan should include how we monitor children when using school-managed devices connected to the internet. This could include:

- Device monitoring using device management software.
- In-person monitoring in the classroom.
- Network monitoring using log files of internet traffic and web access".

At Cavendish Close Infant and Nursery School:

- web filtering is provided by iBoss on our school site and for our school devices.
- overall responsibility is held by the DSL.
- technical support and advice, setup and configuration are from LEAD IT.
- regular checks are made by LEAD IT to ensure filtering is still active and functioning everywhere. These are evidenced in weekly reports shared with the DSL.
- an annual review is carried out as part of the online safety audit to ensure a whole school approach.

At Cavendish Close Infant and Nursery School our school monitoring software is SENSO. Monitoring alerts are checked by our DSL, Mrs C Diffin.

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems.

- Staff at school use the email system provided by Outlook 365 for all school emails. Staff should never use a personal or private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school or child data.

Any systems are centrally managed and administered by the school or LEAD IT. This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed. At school, children have a login for Numbots, it does not have communication facilities.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL.

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If a private account is used for communication

or to store data, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below are given in the social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff code of conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy which can be found on the school website.

Use of generative AI

At Cavendish Close Infant and Nursery School, we acknowledge that generative AI platforms (e.g. ChatGPT, Gemini, Co-Pilot or Adobe Firefly) are becoming widespread. We are aware of and follow the DfE's guidance on this.

- In school, the only approved AI application which staff are allowed to use following advice from LEAD IT is Microsoft CoPilot.
- Teaching staff will receive training on how to use CoPilot effectively and safely, identifying its practical tools.
- Personal or identifiable information should not be used.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some children – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).

Online storage or learning platforms.

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, or teach.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Any new platforms must be approved by LEAD IT.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Mrs C Manners.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with LEAD IT.

Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Cavendish Close Infant School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing images on social media or other platforms without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Cavendish Close Infant School's SM presence

Cavendish Close Infant and Nursery School works on the principle that if we do not manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. We conduct regular checks of privacy and security settings on social media accounts to ensure appropriate access.

Mrs C Manners is responsible for managing our Twitter account.

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school

or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

The school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). Parents may wish to refer to the new Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

The school has an official Twitter account (managed by Mrs C Manners) and will respond to general enquiries about the school but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school.

As outlined in the Acceptable Use Policies, parents and pupils are not allowed to be 'friends' with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Parents and pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public parent or pupil accounts.

Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the pupil or staff member to the school.

Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on digital images and video and permission is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- Children are not allowed to bring their own technology to school.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them during a break in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may request permission from the headteacher and leave their phone in a safe space, out of reach of children, or ask for a message to be left with the school office. This expectation applies to wearable technology too.
- Phones must be kept with personal belongings in a safe cupboard, out of reach of children. They must not be kept in pockets.
- **Volunteers, contractors, governors** should leave their phones in a safe space and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos.

If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member of staff.

- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. We do not allow Apple AirTags or similar devices in school. Please note that it is against the terms and conditions of these products to use them to track children.
- Phones and wearable technology must not be used or viewed when with children.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy or staff code of conduct.

Staff and students have access to Wi-Fi on school devices and activity is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning.

All and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from school

For school trips/events away from school, school staff are allowed to use their personal mobile phone should they need to make contact with emergency services, school, and parents/carers as appropriate. Personal smart technology, including mobile phones, must not be used for any other reason.

Photographs and videos can be taken on school iPads.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher and staff authorised by them have a statutory power to search pupils property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy.

Appendices

1. Acceptable Use Policies (AUPs) for:
    - Pupils
    - Staff, Volunteers and Governors
    - Visitors and Contractors
    - Parents
2. Teaching Online Safety (DfE)
3. Online-Safety Questions from the Governing Board (UKCIS)
4. Letter to parents about filming/photographing/streaming school events
5. Sharing nudes and semi-nudes guidance from UKCIS:
    - How to respond to an incident - overview for all staff
6. NSPCC Whistleblowing Helpline poster
7. Digital family agreement
8. Online Safety Audit