	Online Safety Policy Updated: 03-26 Next Review: 12-26 Prepared by: RYB/PAW/JOH Approved by: TZL

This Policy applies throughout the School from the EYFS to Year 6.

Contents (use the hyperlinks in the headings to access that section)

Head	Taryn Lombard Email: head@cavendish-school.co.uk
Designated Safeguarding Lead (DSL) Online Safety Coordinator (with lead responsibility for filtering and monitoring (in conjunction with the IT Manager)	Josie Hodgson Email: jhodgson@cavendish-school.co.uk For safeguarding related matters: safeguarding@cavendish-school.co.uk
Deputy Designated Safeguarding Leads (DDSLs)	Callum Moore and Maryam Kadhim Email: safeguarding@cavendish-school.co.uk
Nominated governor for safeguarding and online safety, including filtering and monitoring	Alice Gotto Contact details: via the school office
IT Manager with responsibility for filtering and monitoring (in conjunction with the Online Safety Coordinator)	Ryan Bunting Email: itmanager@cavendish-school.co.uk
Computing Coordinator	Paula Webb Email: pwebb@cavendish-school.co.uk
PSHE Coordinator	Krystal Demetriou Email: kdemetriou@cavendish-school.co.uk Victoria Levell (Maternity Cover) Email: vlevell@cavendish-school.co.uk
RSE Coordinator	Sarah Craven Email: scraven@cavendish-school.co.uk

Key people

Key contacts in the Local Borough of Camden

Child Protection Service Manager:
Name: Kurt Ferdinand
Tel: 020 7974 6481

Local Authority Designated Officer (LADO):
Name: Jacqueline Fearon
Contact: 0202 7974 4556
Email: LADO@camden.gov.uk

Camden Children's Contact Service/MASH team:
Manager: Fatima O'Dwyer
Tel: 020 7974 1553/3317

Camden Online Safety Officer:
Name: Jenni Spencer
Tel: 020 7974 2866

Prevent Coordinator/Education Officer:
Name: Jane Murphy
Tel: 020 7974 1008

Introduction

Our pupils are growing up in a world dominated by information and communications technology (ICT) that provides them with access to a wide range of information and increased opportunities for instant communication and social networking. Using the internet and associated devices are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is still constantly changing. Children are often unaware that they are as much at risk online as they are in the real world, and parents and teachers may not be aware of the actions they can take to protect them. We understand that with greater access to technology comes risk and danger to young people and concerns can occur both online and offline simultaneously or separately.

It is, therefore, the school's policy that the educational and social benefits of the internet should be promoted, but that this should be balanced against the need to safeguard children. To achieve this, we have developed an online safety strategy working in partnership with parents. This document sets out how the school helps all stakeholders to recognise the risks and act to help children use the internet and all ICT safely and responsibly.

Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. The table shown in Appendix 5 provides brief details of the various uses of the internet together with their benefits and risks.

As the use of technology is now universal, it is imperative that pupils learn computing skills and that the inherent risks are not used to reduce pupils' use of technology. Further, the educational advantages of computing need to be harnessed to enhance pupils' learning.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for our pupils. There is a danger that pupils may be exposed to illegal, inappropriate or harmful content, such as pornography, fake news or information advocating violence, racism, misogyny, self-harm, suicide, antisemitism,

radicalisation and extremism, illegal and anti-social behaviour and misinformation, disinformation (including fake news) and conspiracy theories, which the pupils are not able to evaluate in a critical manner. Emerging technologies, including artificial intelligence (AI) and generative content platforms, also present new risks, such as the creation and sharing of deepfake or misleading material. Pupils will be taught to critically evaluate digital information and identify trustworthy sources.

Contact

Chat rooms, gaming sites and other social networking sites can be a great source of pleasure but can also pose a real risk to pupils. Pupils may be subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Pupils may not be aware of the danger of publishing or disclosing personal information about themselves, such as contact details that allow them to be identified or located. They may also inadvertently put other pupils at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a pupil (known as online bullying or cyberbullying) or for child-on-child abuse. More details on this can be found on page 13 of this Policy.

Commerce

Pupils are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parents' credit card details, in response to offers for goods or services, without seeing the fraudulent intent. Pupils may also be targeted by online scams, phishing attempts, and in-app purchases that encourage spending or data sharing. Contact via social networking sites can also be used to persuade pupils to reveal computer passwords or other information about the family for the purposes of fraud.

Conduct (or Culture)

Pupils need to be taught to use the internet in a responsible way, as they may put themselves or others at risk by:

- Seeing upsetting or inappropriate images
- Becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- Using information from the internet in a way that breaches copyright laws
- Uploading personal information about themselves and or others, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- Cyberbullying and child on child abuse
- Use of mobile devices for the purposes of sexual harassment, such as the consensual and non-consensual taking and distributing of inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on

to a much wider audience than the child intended

Pupils may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development, and educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable pupils may be at a high degree of risk from such sites. All pupils may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these online. The school also recognises the risks posed by mobile and smart devices and manages these through its IT & Acceptable Use Policy.

Aims

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

- Setting out expectations for all community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping the safeguarding and senior leadership team to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSE) and beyond
- Helping all stakeholders to recognise that online/digital 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
- Facilitating 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's and tomorrow's digital world, to survive and thrive online
- Helping 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 ethos, aims and objectives, and protecting the reputation of the school and profession
    - Establishing 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 for Pupils)
- Use of a safe internet platform that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems. This includes robust filtering and monitoring systems that comply with the Department of Education Filtering and Monitoring Standards for Schools and Colleges (2023)

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

- A culture of safe practice underpinned by a strong framework of online safety policy that

ensures everyone is aware of expected standards of online behaviour

- Children are taught to keep themselves and others safe online and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use

Further help and support

Internal school channels will be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which will be reported in line with our Safeguarding and Child Protection Policy. Any online safety concerns, including potential breaches, harmful content or incidents, should be reported immediately to the DSL or a Deputy DSL. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and the Head will handle referrals to the LA Designated Officer (LADO). The local authority may also offer general support. Training is also available via Educare and LGFL.

This policy works alongside the school's Data Protection Policy and ensures compliance with Data Protection Legislation[1].

Scope

This policy applies to all members of the school community (including teaching, supply and support staff, governors, volunteers, contractors, pupils, 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.

Whole School approach

A successful online safety strategy needs to be inclusive of the whole School community, including teaching assistants and administrative staff, Governors and others, as well as pupils and parents/carers. It applies to the whole school, including the Early Years Foundation Stage. It applies to access to school systems, the internet and the use of technology, using devices provided by the school or personal devices. The strategy has the backing of the Governors, is overseen by the Head and is fully implemented by all staff, including technical and non-teaching staff.

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/s in Appendix 1 of this document that describe individual roles and responsibilities. Please note there is one for all staff which must be read even by those who have a named role in another section.

Staff are aware that online safety is an element of many safeguarding issues, as technology can be used to aid many forms of abuse and exploitation, for example, sexual harassment and cyberbullying, and should be aware of the use of technology in peer-on-peer abuse. Online safety

[1] [1] General Data Protection Regulation (EU 2016/679), the UK Data Protection Act 2018 and related legislation, The Privacy and Electronic Communications Regulations 2003 and the Protection of Freedoms Act 2012.

training is provided to staff on a regular basis and forms part of new staff induction.

It is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

One of the key features of the school's online safety strategy is teaching pupils to protect themselves and behave responsibly while online. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and coordination of online safety education lies with the Head, Online Safety Coordinator and Computing Coordinator, but all staff should play a role in delivering online safety messages
- The Online Safety Coordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum
- Rules regarding safe internet use should be posted in all classrooms and teaching areas where computers are used to deliver lessons and updated regularly to reflect new guidance, apps, or risks
- The start of lessons where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe, including the responsible use of AI tools
- Schools are required to teach about online bullying as part of statutory Relationships Education (primary), Relationships and Sex Education (secondary) and health education (all schools) https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education
- PSHE lessons provide an ideal and statutory framework for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst online
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, including pupils with SEND, looked after children, or those with mental health needs
- Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to

Computing is now a key part of the school curriculum as well as a key element of modern communications technology that is widely used, and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment. Guidance on planning technology in schools can be found here: Plan technology for your school - GOV.UK
The Cavendish has an online safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- Promote the use of technology within the curriculum

- Protect all pupils from harm regardless of age, race, gender and other protected characteristics
- Safeguard staff in their contact with pupils and their own use of the internet
- Ensure the School fulfils its duty of care to pupils
- Provide clear expectations for staff and pupils on acceptable use of the internet

The Cavendish School ensures the following:

- A safe internet platform that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems. This includes robust filtering and monitoring systems that comply with the Department of Education filtering and monitoring standards for schools and colleges
- A culture of **safe practice** underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of online behaviour
- That pupils are **taught to keep themselves and others safe** online and use technology responsibly; this should be achieved by working in partnership with parents and raising awareness of the potential risks of internet use

We have established a carefully sequenced curriculum for online safety that 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, the curriculum now includes explicit teaching on digital literacy, critical thinking, mental health, and wellbeing in online contexts. Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole-school approach, including tailoring support to vulnerable pupils.

https://www.gov.uk/government/publications/teaching-online safety-in-schools/teaching-online safety-in-schools

The following subjects have the clearest online safety links:

- Relationships and Sex Education (RSE) and Health, and Personal Social Health Economic (PSHE) Education
- Computing
- Citizenship

However, as stated in the role descriptors in Appendix 1, 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 curriculum/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Through assemblies and displays around school, our pupils learn about the 4Cs of online safety Content, Conduct, Contact and Commerce. They are also reminded to follow rules to keep themselves and others safe.

Pupils know that if they are worried about something that happens online, they should report it to a trusted adult. They are encouraged to take a screenshot or other evidence, where safe to do so, and to report immediately to a staff member. If reported to school, we will investigate it and follow our Behaviour Policy. Parents will be informed of the incident so that all parties are aware of the concern raised. This will help parents have follow-up conversations with their children and understand any sanctions that are given. The School is also aware of DfE guidance on generative AI safety expectations to ensure the safe and appropriate use of AI products within the school environment: Generative AI: product safety expectations - GOV.UK

Acceptable Use Agreements (AUA)

All pupils, parents, staff, volunteers and governors are expected to read and abide by an agreement regarding the acceptable use of the school's online systems. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only or for the purpose of fulfilling the duties of an individual's role. We monitor all school-owned devices as well as the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices 2 and 3.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff will encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites. "Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online" (KCSIE 2024).

Equally, all staff will carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g., disinformation, misinformation and fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law.

At the Cavendish 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/schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of self-image and identity, online

relationships, online reputation, online bullying, managing online information, health, wellbeing and lifestyle, privacy and security, and copyright and ownership. This review now also considers risks associated with generative AI, radicalisation, and sexual harassment online.

This is done within the context of an annual online safety audit, which is a collaborative effort led by the Online Safety Coordinator.

- See Computing Subject Policy

Pupils with special educational needs and disabilities (SEND)

Pupils with learning difficulties or disabilities may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. The School has a flexible and personalised approach to online safeguarding for these pupils in order to meet their needs.

SEND Coordinators are responsible for providing extra support for these pupils and will:

- Link with the Online Safety Coordinator/Computing Coordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND
- Where necessary, liaise with the Online Safety Coordinator and the IT Manager to discuss any requirements for further safeguards to the School IT system or tailored resources and materials in order to meet the needs of pupils with SEND
- Ensure that the School's Online Safety Policy is adapted to suit the needs of pupils with SEND
- Be aware that some pupils with SEND may not have the cognitive understanding to differentiate between fact and fiction online and may require scaffolded teaching to understand online risks, including sexual content, scams, and misinformation
- Liaise with parents and other relevant agencies in developing online safety practices for pupils with SEND
- Keep up to date with any developments regarding emerging technologies and online safety and how these may impact pupils with SEND

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSE and Citizenship).

General 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 err on the side of talking to the Designated Safeguarding Lead 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 (particularly relating to bullying and sexual harassment and violence).

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

- Safeguarding and Child Protection Policy
- Anti-bullying Policy for Pupils
- Behaviour Policy
- Capability and Disciplinary Policy
- Capability and Disciplinary Policy for Employees on Probation
- Code of Conduct for Other Adults in Supervision of Pupils Who Are Not Employees of the School
- Code of Conduct for School Employees
- Computing Subject Policy (incl. Acceptable Use Agreements for pupils)
- Data Protection Policy
- IT & Acceptable Use Policy
- Prevent Policy
- Privacy Notice
- Social Media Policy
- Taking, Storing and Using Images of Pupils Policy
- Whistleblowing Policy

This school commits to taking all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school and will impact pupils' wellbeing, mental health, and behaviour. 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 Coordinator/ Designated Safeguarding Lead on the same day; where clearly urgent, it will be reported by the end of the lesson.

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

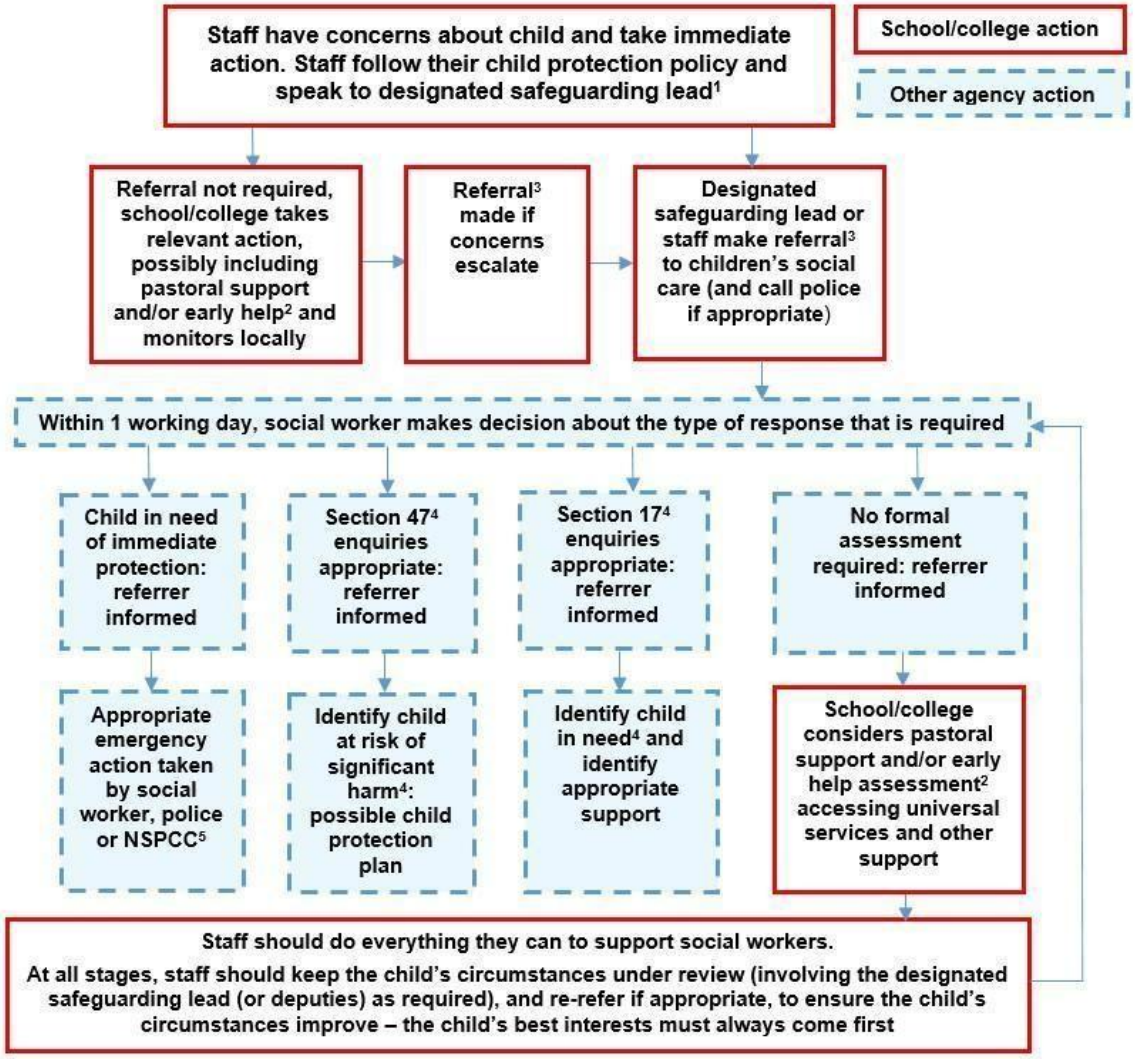
The school will actively seek support from other agencies as needed (i.e., the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for Headteachers and school staff February 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents We 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 (particular procedures are in place for sexting and upskirting; see sections below).

Behaviour in Schools - Advice for headteachers and school staff Feb 2024 (publishing.service.gov.uk)

The school will evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation, etc. and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart is taken from Keeping Children Safe in Education 2025 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



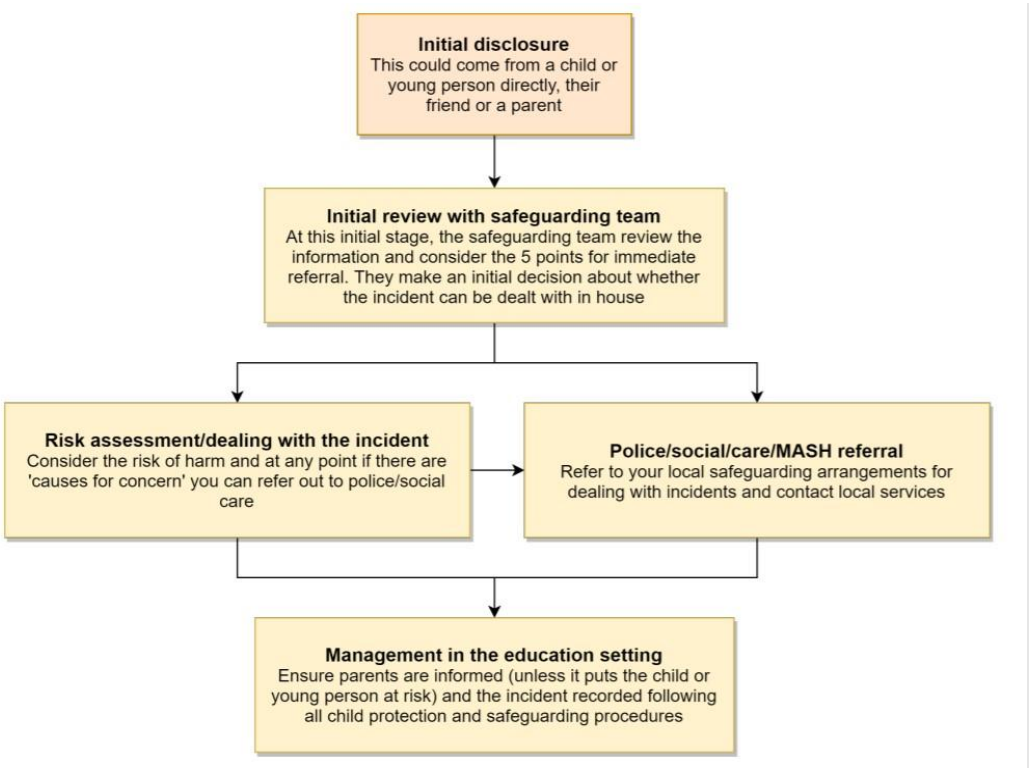
Sharing nudes and semi-nudes (formerly "sexting")

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on **sharing nudes and semi-nudes: advice for education settings** to avoid unnecessary criminalisation of children. **NB – where one of the parties is over 18, this is no longer youth-produced sexual imagery but may constitute child sexual abuse.**

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

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 Coordinator 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, copy, print, share or delete the image or ask anyone else to do so; rather, they must report immediately to the DSL.

The school DSL will, in turn, use the full guidance document, sharing nudes and semi-nudes: advice for education settings to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involve sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting for children under 18 is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at: sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now 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, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, also known as Cyberbullying, is defined as the use of technology, such as email and social networking sites, to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows the distribution of hurtful comments and material to a wide audience.

Online bullying, including incidents that take place outside school or from home, will be treated like any other form of bullying. All incidents will be dealt with under the school's behaviour policy, anti-bullying policy and the child-on-child abuse guidance:

https://cscp.org.uk/wp-content/uploads/2022/09/Child-on-child-abuse-and-sexual-violence-guidance-for-schools-2022.pdf

- School anti-bullying and behaviour policies and IT and acceptable use agreements cover the issue of online bullying and set out clear expectations of behaviour and sanctions for any breach
- Any incidents of online bullying should be reported to the Online Safety Coordinator, who will record the incident on the incident report form and ensure that the incident is dealt with in line with the School's Anti-bullying Policy for Pupils. Incidents will be monitored and the information used to inform the development of the School's Anti-bullying Policy for Pupils
- Where incidents are extreme, for example, threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police, as in these cases, the bullying may be a criminal offence
- As part of online safety awareness and education, pupils will be told of the 'no tolerance' policy for online bullying and encouraged to report any incidents to their teacher
- Pupils will be taught:
    - To only give out mobile phone numbers and email addresses to people

they trust
    - To only allow close friends whom they trust to have access to their social networking page
    - Not to send or post inappropriate images of themselves
    - Not to respond to offensive messages
    - To report the matter to their parents and teacher immediately
- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the pupil as evidence

Any action taken on online bullying incidents must be proportional to the harm caused, and educational/restorative responses may be more appropriate than sanctions in some cases. This may be facilitated by the School Council, the Wellbeing Champions or the Digital Leaders.

Child-on-child sexual violence and sexual harassment

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases, these actions may be harmful or abusive or may constitute sexual harassment or online bullying and because of the nature of online activities, this can lead to more widespread harm and repeat victimisation.

Keeping Children Safe in Education places a duty on schools to respond to any incidents of online sexual harassment, such as:

- Consensual and non-consensual sharing of nude and semi-nude images
- Sexualised online bullying
- Unwanted sexualised comments and messages
- Sexual exploitation, coercion or threats
- Coercing others into sharing images or performing acts online that they are not comfortable with

School staff should refer to the child-on-child abuse and sexual violence and harassment guidance for schools and colleges for further details on what actions need to be taken in response to online sexual harassment.

https://cscp.org.uk/wp-content/uploads/2022/09/Child-on-child-abuse-and-sexual-violence-guidance-for-schools-2022.pdf

Any incident of sexual harassment or violence (online or offline) will be reported to the DSL, who will follow the full guidance. Staff work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. We 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.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour. These incidents are treated on a case-by-case basis and we work with parents to raise awareness and explore access to such content online, which may be influencing their child's views.

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 policies (Code of Conduct for staff and Computing Subject policy for pupils. 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/handbook.

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, etc.

Further to these steps, the school reserves the right to withdraw, temporarily or permanently, any or all access to such technology.

Artificial Intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft CoPilot. We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. We will treat any use of AI to bully pupils in line with our Anti-bullying Policy and Behaviour Policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should seek permission from our Head or Senior Deputy Head where new AI tools are being used by the school and ensure appropriate filtering, monitoring and usage controls aligned with DfE's Generative AI product safety expectations.

Online safety incident reporting

All significant or complex incidents and complaints relating to online safety and unacceptable internet use will be reported to the Online Safety Coordinator in the first instance. All incidents, whether involving pupils or staff, must be recorded by the DSL on the online safety incident report form (appendix 4).

A copy of the incident record will be emailed to Camden's Designated Online Safety Officer.

Where the incident or complaint relates to a member of staff, the matter must always be referred to the Head for action under staff conduct policies for low-level incidents or consideration given to

contacting the LADO under the CSCP guidance on dealing with allegations against staff where this is appropriate. Incidents involving the Head should be reported to the Chairs of the Board of Governors.

The school's DSL will keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system and use these to update the online safety policy.

Online safety incidents involving safeguarding issues, for example, contact with inappropriate adults, will be reported to the Designated Safeguarding Lead, who will make a decision as to whether or not to refer the matter to the police and/or Children's Safeguarding and Family Help, in conjunction with the Head.

Although it is intended that online safety strategies and policies should reduce the risk to pupils whilst online, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

Social media incidents

These are also governed by the school's Acceptable Use Agreements (Code of Conduct, IT & Acceptable Use Policy) and the Social Media Policy.

Breaches will be dealt with in line with the school Behaviour Policy (for pupils) or Code of Conduct (for staff or other adults).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the 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.

Confidentiality, data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's Data Protection and Cybersecurity procedures. It is important to remember that effective safeguarding depends on the proper management of data protection and cybersecurity. Schools are reminded of this in KCSIE, which also refers to the DfE Standards of Cybersecurity.

The school recognises that data protection obligations do not prevent or limit the sharing of information for safeguarding purposes. 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 2023, "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."

- The School will ensure that all data held on its IT systems is held in accordance with data protection legislation[2]. Data will be held securely and password-protected, with access given only to staff members on a 'need to know' basis
- Pupil data that is being sent to other organisations will be password-protected and sent via a safe and secure system. Any breaches of data security should be reported to the Head of HR & Compliance immediately. They will record the security breach and decide whether it warrants reporting to the Information Commissioner's Office and/or the individuals affected

In the areas where the School uses CCTV, a notice is displayed in a prominent place to ensure that staff and pupils are aware and recordings will only be accessed in accordance with relevant permissions and legal requirements.

Appropriate filtering and monitoring

KCSIE requires schools to ensure "appropriate" web filtering and monitoring systems that protect children online without unreasonably restricting access to educational resources.

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the Designated Safeguarding Lead now has lead responsibility for filtering and monitoring.

The governing body retains strategic oversight of filtering and monitoring, ensuring that systems meet the DfE Filtering and Monitoring Standards. The DSL, alongside the IT Manager, hold operational responsibility for ensuring systems remain effective and embedded in safeguarding practice.

The school follows the new DfE filtering and monitoring standards, which require us 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

[2] **"Data Protection Legislation"** means any data protection legislation from time to time in force in the UK including the Data Protection Act 2018 and the UK General Data Protection Regulation (or any successor legislation).

All staff are aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential over-blocking. They can submit concerns at any point via email and will be asked for feedback at the time of the regular checks, which will now take place.

All staff receive annual training and regular updates on how the school's filtering and monitoring systems work, including what is blocked, how monitoring operates and how to report technical or safeguarding concerns linked to these systems.

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

At The Cavendish School:

- Web filtering is provided by Smoothwall on school site and for school devices used in the home
- Changes can be made by the IT Manager
- Overall responsibility is held by the DSL, with further support from the IT Manager and the Head
- The governing body maintains strategic oversight of filtering and monitoring arrangements
- Technical support and advice, setup and configuration are from the IT Manager
- Regular checks are made half-termly by the IT Manager to ensure filtering is still active and functioning everywhere
- An annual review is carried out by the Online Safety Coordinator
- An annual filtering and monitoring risk assessment is completed in line with DfE standards, taking into account pupil age, device use and safeguarding vulnerabilities
- Filtering and monitoring apply to all school-owned devices, whether used on-site or at home

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet-connected devices" and may include:

1. Physically monitoring by staff watching the screens of users
2. Live supervision by staff on a console with device management software
3. Network monitoring using log files of internet traffic and web access
4. Individual device monitoring through software or third-party services

At The Cavendish School, we have decided that options 1,3 and 4 are appropriate because of the ages of the children we work with.

Any monitoring alerts indicating potential safeguarding concerns are triaged by the DSL (or deputy), logged and responded to in line with the Safeguarding and Child Protection Policy.

Any attempt by a pupil to bypass filtering or monitoring systems is treated as a safeguarding concern and may also be dealt with under the Behaviour Policy.

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

Authorised systems

- Pupils at this school can communicate with staff using Google Classroom on comments related to their work. This is monitored by the class teacher.
- Pupils at this school do not currently have access to emails
- Staff at this school use their school email account only to communicate with parents

Email, School Comms and Google Classroom are the only authorised means of electronic communication between staff and pupils/staff and parents (in both directions). Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head (if by a staff member).

We use social media and our school website to share information with parents about past and future events in school. Comments on school social media accounts are monitored by the Admissions and Marketing Manager.

Any systems above are centrally managed and administered by the school or authorised by the IT Manager (i.e., they can be monitored/audited/viewed centrally; are not private or linked to private accounts). 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.

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 must always be followed, and only authorised systems are to be used
- 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 Head and Governors have delegated the day-to-day responsibility of updating the content of the website to the Admissions &

Marketing Manager. The site is managed by/hosted by MSO.

Cloud platforms

For online safety, basic rules of good password hygiene ("treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The Data Protection Lead and IT Manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPL approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open-access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g., a private Gmail account or Google Drive and those belonging to a managed educational domain)

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 are asked to opt in or out of internal use of images and external use of images separately.

Parents who choose to opt out can make any exclusions necessary, e.g. their child can be photographed in group activities only. However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example, for internal identification, if they are included incidentally in CCTV or a photograph, or if a photo is taken of children from the back and images are non-recognisable).

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

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

Full information can be found in the School's Taking, Storing and Using Images of Pupils Policy.

All staff are governed by their contract of employment, the Safeguarding and Child Protection Policy and the Code of Conduct, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At The Cavendish School, no member of staff will ever use their personal phone to capture photos or videos of pupils. Staff members have access to iPads, which will be taken on educational visits to capture photos/videos. Photos are stored on various platforms, including: media drive, shared drive, iCloud, iPad, shared folder on shared network.

We encourage young people to think about their online reputation and digital footprint. Pupils are taught about how images can be manipulated in their computing lessons. Pupils are advised to be very careful about placing any personal photos on online platforms. 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 is subject to bullying or abuse.

Our social media presence

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.

The Admissions & Marketing Manager is responsible for managing our X-Twitter/Instagram/Facebook accounts and checking our Google reviews. They follow the guidance in the LGfL/Safer Internet Centre online reputation management document.

Staff, pupils and parents' social media 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 agreements, 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. Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. However, 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/students 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.

Although the school has an official Facebook/X-Twitter/Instagram account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, is not appropriate for school use.

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.

* Exceptions may be made, e.g., for pre-existing family links, but these must be approved by the Head, 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 (if by a child) or to the Head (if by a staff member).

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, trust 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.

The statements of the Acceptable Use Agreements (AUAs), which all members of the school community have signed, are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

AUAs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUAs 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. Pupil AUAs can be found in Appendices 2 & 3 to this policy.

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

- Pupils in Year 6 are allowed to bring mobile phones in for emergency use if walking home alone. Phones are collected in the morning, switched off and returned at the end of the day. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to a sanction and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies
- Staff should not use their personal mobile devices when in class with pupils or in shared School areas (e.g., corridors, playground) during the course of the School day. Specific provisions for personal mobile devices apply to EYFS staff in accordance with the School's Safeguarding and Child Protection Policy. Full information can be found in the School's IT & Acceptable Use Policy. Volunteers, contractors and governors should leave their phones in their bags or pockets and turn them 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 Head should be sought (the Head 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 bags or pockets and turn them 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. When at school events, please refer to the digital images and video section of this document on page 20. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office

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 AUAs, Behaviour Policy/ Code of Conduct for staff
- Wifi is accessible to staff for school-related internet use/limited personal use within the framework of the acceptable use policy. All such use is monitored
- We also have a guest wifi, which access is given upon request to contractors, guests and volunteers. All connected devices are subject to our filtering and monitoring systems
- All devices connected to the school network, including guest wifi, are subject to filtering and monitoring in line with DfE standards.

Trips and events away from School

For school trips/events away from school, the lead teacher will use their personal phone in an emergency or to notify the school office if there is a delay in returning to school. Staff phone numbers are not shared with parent volunteers, but staff contact information may be shared

between staff on the trip in cases of emergency. Parent volunteers are provided with the school's contact number in the information pack they are given on the trip (which includes the outline of the day and the parent code of conduct). If a staff member needs to contact a parent regarding their child, they will ensure that the number is hidden to avoid a parent or pupil accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Head 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 on our school website.

Linked policies

- Safeguarding and Child Protection Policy
- Anti-bullying Policy for Pupils
- Behaviour Policy
- Code of Conduct
- Code of Conduct for Other Adults in Supervision of Pupils Who Are Not Employees of the School
- Computing Subject Policy
- Data Protection Policy
- IT and Acceptable Use Policy
- Social Media Policy
- Taking, Storing and Using Images of Pupils Policy

APPENDIX 1 – ROLES AND RESPONSIBILITIES

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the "all staff" section as well as any other relevant to specialist roles.

Roles:

- All staff
- Head
- Designated Safeguarding Lead/Online Safety Coordinator
- Governing Body, led by the Online Safety/Safeguarding Link Governor
- PSHE/RSE Leads
- Computing Coordinator
- IT Manager
- Data Protection Lead (DPL)
- Volunteers and contractors (including peripatetic teachers)
- Pupils
- Parents/carers
- External groups, including FOC (Friends of Cavendish)

All staff

All staff will sign and follow the IT & Acceptable Use Policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct, staff handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the Designated Safeguarding Lead, 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 and avoiding scaring, victim-blaming language.

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- Adhering to the school's Online Safety Policy and IT & Acceptable Use Policy
- Communicating the school's Online Safety Policy and IT & Acceptable Use Policy to pupils
- Keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- Planning use of the internet for lessons and researching online materials and resources
- Reporting breaches of internet use to the Online Safety Coordinator
- Recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example, referral to the Online Safety

Coordinator
- Teaching the online safety and digital literacy elements of the new curriculum
- Keeping up to date with emerging online risks, including AI-driven tools, social media trends and gaming platforms

Head – key responsibilities

Headteachers have ultimate responsibility for online safety issues within the school, including:

- The overall development and implementation of the school's Online Safety Policy and ensuring the security and management of online data
- Ensuring that online safety issues are given a high profile within the school community
- Linking with the board of governors and parents and carers to promote online safety and forward the school's online safety strategy
- Ensuring online safety is embedded in staff induction and training programmes
- Deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety
- Ensuring compliance with KCSIE and DfE Filtering and Monitoring Standards

Online Safety Coordinator/Designated Safeguarding Lead– key responsibilities

The DSL will "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). Ensure "an effective whole school approach to online safety" in line with KCSIE.

The Online Safety Coordinator should have the authority, knowledge and experience to carry out the following:

- Develop, implement, monitor and review the school's Online Safety Policy
- Ensure that staff and pupils are aware that any online safety incident should be reported to them
- Ensure online safety is embedded in the curriculum
- Provide the first point of contact and advice for school staff, governors, pupils and parents
- Liaise with the school's IT Manager, the Head and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents, emerging risks and arising problems and that the school has appropriate filtering and monitoring systems in line with DfE guidance
- Assess the impact and risk of emerging technology in consultation with the **Computing Coordinator and the IT Manager** and the learning platform providers
- Maintain a log of internet-related incidents and coordinate investigations into breaches
- Report termly to the board of governors on the implementation of the school's online safety strategy

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated safeguarding lead for the school, who will

decide whether or not a referral should be made to Children's Safeguarding and Family Help or the Police.

Online Safety and Safeguarding Link Governor - key responsibilities (quotes are taken from KCSIE)

- Approve this policy and strategy and subsequently review its effectiveness
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and 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
- Liaise with the IT Manager, Online Safety Coordinator and service providers to annually review school IT filtering and monitoring systems to check their effectiveness and ensure that the school leadership team are aware of what provision is in place and how to escalate any concerns
- 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 Coordinator/DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPL, DSL and head 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 and that all working directly with children have also read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also 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."

PSHE/RSE Coordinators – 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 PSHE/Relationships education, relationships and sex education (RSE) and health education 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] tests, written assignments or self-evaluations, to capture

progress" –LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net] to complement the computing curriculum
    - Work closely with the DSL/OSC and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE/RSE
    - Note that an RSE policy should be included on the school website
    - Work closely with the Computing Coordinator to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Coordinator – 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
    - Look at the RSE curriculum to avoid overlap but ensure a complementary whole-school approach
    - Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within computing
    - Collaborate with the IT Manager and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

IT Manager – key responsibilities

- As listed in the 'all staff' section, plus:
    - Maintain and monitor the School internet system, including anti-virus and filtering and monitoring systems in line with DfE standards
    - Carrying out monitoring and audits of networks and reporting breaches to the Online Safety Coordinator
    - Support any subsequent investigation into breaches and preserving any evidence
    - Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology
    - 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
    - Monitor the use of school technology, online platforms and social media presence and ensure that any misuse/attempted misuse is identified and reported in line with school policy

Data Protection Lead (DPL) – key responsibilities

- Alongside those of other staff, provide data protection expertise and training and support the DP 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 2023, "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 also monitored and audited

Volunteers and contractors (including peripatetic teachers) - key responsibilities

- Read, understand, sign and adhere to an acceptable use agreement (AUA) – when the School's IT systems are being used
- Report any concerns, no matter how small, to the Designated Online Safety Coordinator
- 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

Pupils - key responsibilities

- Read, understand, sign and adhere to the pupil acceptable use agreement. This is done in lesson time with teacher support to read and understand the statements

Working with parents

It is essential that schools involve parents in the development and implementation of online safety strategies and policies; most pupils will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at School.

Therefore, parents need to know about the risks so that they are able to continue online safety education at home and regulate and supervise their children's use as appropriate to their age and understanding.

The Computing Coordinator attends the beginning-of-year curriculum meetings to provide support and guidance to parents, ensuring they are well-informed about online safety. She remains available throughout the year to offer advice and assistance to families, recognising that keeping children safe online is a shared responsibility and partnership between school and home. Online safety resources are reviewed and updated regularly, and these materials are shared with parents to help them stay informed and confident in supporting their children's digital wellbeing.

The Head, Board of Governors and the Online Safety Coordinator should consider what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing

online safety messages at home. Parents are provided with information on the School's IT and Acceptable Use Policy and Online Safety Policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the School as well as the School's expectations regarding their behaviour. There will be regular communication with parents on these matters via the weekly newsletter and weekly mail outs.

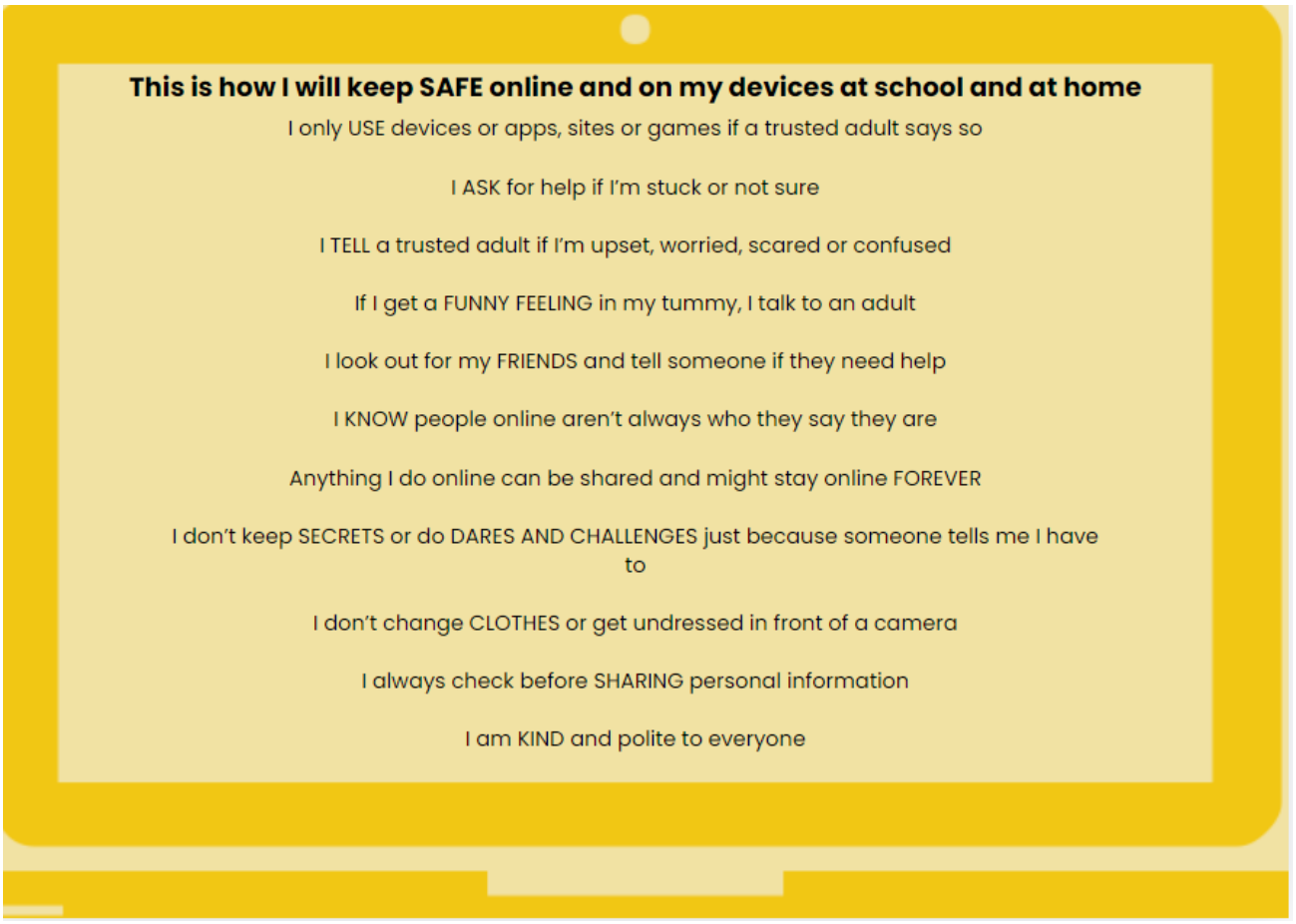
Key responsibilities

- Read the pupil AUA in and encourage their children to follow it

Other visitors - key responsibilities

- Any external individual/organisation will sign an acceptable use agreement as part of the visitor code of conduct, 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 others' 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

APPENDIX 2
Key Stage 1: Acceptable Use Agreement



APPENDIX 3

Key Stage 2: Acceptable Use Agreement

I ask permission – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.

I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game. If I get a funny feeling, I talk about it.

I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

I learn online – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.

I learn even when I can't go to school (e.g. covid isolation)– I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom when I am online. I don't expect teachers to behave differently online. If I get asked or told to do anything that I would find strange in school by anyone including a teacher, I will tell another teacher or ask my trusted adult to do so.

I am a good friend online and part of a community – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening I will tell my trusted adults.

I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

I tell my parents/carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

I say no online if I need to – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

I am creative online – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.

I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.

I am a researcher online – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult

I am a rule-follower online – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.

I follow age rules – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable.

I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

I am not a bully – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

I respect people's work – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.

I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I must not share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

I know new online friends might not be who they say they are and I understand that it can be very unsafe to meet with friends I make online – I am careful when someone wants to be my friend online. I will check with a parent/carer before I arrange to meet an online friend and would never meet them without a trusted adult.

I don't do live videos (livestreams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

I keep my body to myself online – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

I am aware that my digital footprint is the record of all my interactions online – I know anything I do can be shared and might stay online forever.

APPENDIX 4

ONLINE SAFETY INCIDENT REPORT FORM (CAMDEN TEMPLATE)

This form should be kept on file and a copy emailed to Camden's online safety officer at jenni.spencer@camden.gov.uk

School details:

Name of school _____

Address _____

Name of Online Safety Coordinator _____

Contact details _____

Details of incident _____

_____

Date happened _____

Time _____

Name of person reporting incident _____

If not reported, how was the incident identified?

Where did the incident occur?

□ In school setting □ Outside school setting

Who was involved in the incident?

□ Pupil □ Staff member □ Other (please specify)

Type of incident:

□ Bullying or harassment (online bullying)
□ Deliberately bypassing security or access
□ Hacking or virus propagation
□ Racist, sexist, homophobic religious hate material
□ Terrorist material
□ Drug/bomb making material
□ Child abuse images
□ Online gambling
□ Soft core pornographic material
□ Illegal hard core pornographic material
□ Other (please specify)

Description of incident

Nature of incident

□ **Deliberate access**

Did the incident involve material being:

□ Created	□ Viewed	□ Printed
□ Shown to others	□ Transmitted to others	□ Distributed

Could the incident be considered as:

□ Harassment	□ Grooming	□ Online bullying	□ Breach of AUA

□ **Accidental access**

Did the incident involve material being:

□ Created	□ Viewed	□ Printed
□ Shown to others	□ Transmitted to others	□ Distributed

Action taken

□ **Staff**

□ Incident reported to Head/SLT

□ Advice sought from Children's Safeguarding and Social Work

□ Referral made to Children's Safeguarding and Social Work

□ Incident reported to police

□ Incident reported to social networking site

□ Incident reported to IT Manager

□ Disciplinary action to be taken

□ Online Safety Policy to be reviewed/amended

Please detail any specific action taken (i.e. removal of equipment)

_____

_____

□ **Pupil**

□ Incident reported to Head/SLT

□ Advice sought from Children's Safeguarding Services and Social Work

□ Referral made to Children's Safeguarding Services and Social Work

□ Incident reported to police

□ Incident reported to social networking site

□ Incident reported to IT Manager

□ Pupil's parents informed

□ Disciplinary action to be taken

□ Pupil debriefed

□ Online Safety Policy to be reviewed/amended

Outcome of incident/investigation

_____

_____

_____

APPENDIX 5: DESCRIPTION OF ONLINE APPLICATIONS

Technology/ Application	Description/ Usage	Benefits	Risks
Internet	• Enables the storage, publication and retrieval of a vast range of information • Supports communications systems	• Provides access to a wide range of educational materials, information and resources to support learning • Enables pupils and staff to communicate widely with others • Enhances schools management information and business administration systems	• Information is predominantly for an adult audience and may be unsuitable for pupils • The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information • Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites
Email	• Allows written communications over the network and the ability to attach documents	• Enables exchange of information and ideas and supports collaborative working • Enhances written communications skills • A good form of communication for pupils with some disabilities	• Difficulties controlling contacts and content • Use as a platform for bullying and harassment • Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems • Hacking • Unsolicited mail
Chat/instant messaging/ gaming	• Chat rooms allow users to chat online in real time in virtual meeting places with a number of people • Instant messaging allows real- time chat for 2 or more people privately with no-one else able to join. Users have control over who they contact through 'buddy lists'	• Enhances social development by allowing pupils to exchange experiences and ideas and form friendships with peers • Use of pseudonyms protects the pupil's identity • Moderated chat rooms can offer some protection to pupils	• Anonymity means that pupils are not aware of who they are really talking to • Chat rooms may be used by predatory adults to contact, groom and abuse pupils on- line • Risk of pupils giving away personal information that may identify or locate them • May be used as a platform to bully or harass

Social networking sites	• Online communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging • It allows creation of individual profiles • Users can develop friends lists to allow access to individual profiles and invite comment	• Allows pupils to network with peers and join forums to exchange ideas and resources • It provides a creative outlet and improves computer studies skills	• Open access means pupils are at risk of unsuitable contact • Risk of pupils posting unsuitable material online that may be manipulated to cause them embarrassment or distress • Pupils may post personal information that allows them to be contacted or located • May be used as a platform to bully or harass
File sharing (peer-to-peer networking)	• Allows users to share computer capability, networks and file storage • Used to share music, video and other materials	• Allows pupils to network within a community of peers with similar interests and exchange materials	• Illegal download and copyright infringement • Exposure to unsuitable or illegal materials • Computers are vulnerable to viruses and hacking
Mobile phones and multi-media equipment	• Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email	• Provide pupils with a good means of communication and entertainment • They can also keep pupils safe and allow them to be contacted or stay in contact	• Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging • Risk from violent crime due to theft • Risk of online bullying via mobile phones