Online Safety Policy

Dover College



Owner:	DSL & Assistant Head Co-Curricular	Date: August 2026
Approved By:	Chair of Council	Date: August 2026
Review Frequency	Annually	
Last reviewed on:	August 2026	
Next review due by:	August 2027	

Contents

1. Aims

2. Legislation and guidance

3. Roles and responsibilities

4. Educating pupils about online safety

5. Educating parents/carers about online safety

6. Cyber-bullying

7. Acceptable use of the internet in school

8. Pupils using mobile devices in school

9. Staff using work devices outside school

10. How the school will respond to issues of misuse

11. Training

12. Monitoring arrangements

13. Links with other policies

1. Aims

Our school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology such as smartphones, smart watches, smart glasses and other wearable devices (which we refer to as 'mobile phones', as defined in section 1.1 of the Mobile Phone Policy).

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk
Our approach to online safety is based on the four categories of risk set out in section 6 of the Safeguarding and Child Protection Policy: content, contact, conduct and commerce.

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.
- Contact – being subjected to harmful online interaction with other users, or with generative AI applications that simulate this (such as chatbots and AI companion apps), for example 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.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), including images generated or altered using AI, sharing other explicit images, and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2026 (KCSIE), which is in force from 1 September 2026, and on the following guidance and advice:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships Education, Relationships and Sex Education (RSE) and Health Education: statutory guidance (2025), in force from 1 September 2026
- Searching, screening and confiscation
- Mobile phones in schools: statutory guidance (statutory from 29 June 2026, followed by schools from 1 September 2026)
- Filtering and monitoring standards for schools and colleges
- Cyber security standards for schools and colleges
- Generative artificial intelligence (AI) in education, including the DfE's generative AI product safety expectations
- UK Council for Internet Safety (UKCIS): Sharing nudes and semi-nudes: advice for education settings working with children and young people

It also reflects the Prevent duty guidance and the DfE's advice on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Equality Act 2010, the Online Safety Act 2023, and data protection law (the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025). In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so, and section 36 of the Children's Wellbeing and Schools Act 2026, which requires schools to have regard to the DfE's mobile phones guidance. The full statutory and regulatory framework within which this policy operates, including the Education (Independent School

Standards) Regulations 2014 and the National Minimum Standards for Boarding Schools, is set out in section 1.2 of the Safeguarding and Child Protection Policy.

3. Roles and responsibilities

3.1 Governors

Governors have overall responsibility for monitoring this policy and holding the Headmaster to account for its implementation.

Governors will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

Governors will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

Governors will receive regular reports on online safety, including training and the operation of filtering and monitoring, from the Designated Safeguarding Lead. Reports to governors will not include details of individual pupil situations or identifying features of families.

Governors should ensure children are taught how to keep themselves and others safe, including keeping safe online.

- Governors have overall strategic responsibility for the school's filtering and monitoring approaches. The named roles, the arrangements for meeting the DfE filtering and monitoring standards, the annual review, and the logging and recording of system checks are set out in section 6.3 of the Safeguarding and Child Protection Policy. Governors will receive assurance that those arrangements have been carried out.
- Governors are also responsible, with the DSL and the safeguarding governor, for ensuring that the school meets the DfE cyber security standards for schools and colleges as part of its wider safeguarding responsibilities, as set out in section 6.4 of the Safeguarding and Child Protection Policy.

The governor who oversees online safety is the nominated safeguarding governor.

All governors will:

- Ensure they have read and understand this policy.

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (AUP policy).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headmaster

The Headmaster is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL), deputies and wider Safeguarding Team are set out in the Safeguarding and Child Protection Policy and on posters displayed throughout the school.

The DSL is also the school's Online Safety Lead and the member of the senior leadership team with operational responsibility for filtering and monitoring (section 6.3.1 of the Safeguarding and Child Protection Policy). The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headmaster in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headmaster and governors to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Overseeing and acting on filtering and monitoring reports, any safeguarding concerns they identify, and checks to the filtering and monitoring systems, including reviewing monitoring logs at Online Safety Group meetings
- Working with the Network Manager to make sure the appropriate systems and processes are in place
- Working with the Headmaster, Network Manager and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the Safeguarding and Child Protection Policy
- Ensuring that online safety incidents with a safeguarding dimension are recorded on My Concern, and that other incidents are recorded on the appropriate system, in line with section 7 of the Behaviour and Discipline Policy – Senior School
- Ensuring that incidents of cyber-bullying are recorded on the College Bullying Log and dealt with in line with the Anti-Bullying Policy and the Behaviour Policy, and that any which raise a safeguarding concern or may constitute child-on-child abuse are also recorded on My Concern
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headmaster and/or governors
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

- Leading the annual review of the school's approach to online safety, supported by a risk assessment, as set out in section 6.9 of the Safeguarding and Child Protection Policy

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network Manager leads the IT staff referred to in section 6.3 of the Safeguarding and Child Protection Policy and is responsible for:

- Maintaining the filtering and monitoring systems and providing filtering and monitoring reports, in line with the arrangements and responsibilities set out in section 6.3 of the Safeguarding and Child Protection Policy.
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Completing technical actions identified through filtering and monitoring checks and reviews, and supporting the termly system checks and the annual review set out in section 6.3.2 of the Safeguarding and Child Protection Policy
- Supporting the school to meet the DfE cyber security standards for schools and colleges, including secure access, account permissions and multi-factor

authentication where applicable (section 6.4 of the Safeguarding and Child Protection Policy)
- Reporting any safeguarding concern identified through filtering, monitoring or other technical work to the DSL via My Concern, and any concern relating to a member of staff to the Headmaster (or to the Chair of Council where the concern relates to the Headmaster)
- Supporting the DSL and pastoral staff with technical information when incidents of cyber-bullying or other misuse are investigated

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (see AUP) , and ensuring that pupils follow the school's terms on acceptable use (see AUP)
- Working with the DSL to ensure that online safety incidents with a safeguarding dimension are recorded on My Concern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported, recorded on the College Bullying Log and dealt with in line with the Anti-Bullying Policy and the Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

- Reporting any online safety concern about a pupil to the DSL without delay, and any concern about the conduct of an adult to the Headmaster, in line with the Safeguarding and Child Protection Policy
- Never viewing, copying, forwarding, saving, printing or deleting suspected nude or semi-nude imagery of a child (including AI-generated imagery), and reporting it to the DSL immediately
- Reporting to the DSL any concern that filtering or monitoring may not be working effectively, or is unreasonably restricting teaching and learning
- Applying the Mobile Phone Policy consistently, including its expectations for staff use of personal devices (see section 8)

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headmaster of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet

- Support the Mobile Phone Policy, and contact their child during the school day through the College office rather than directly on a personal device

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see AUP).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In the **Early Years Foundation Stage**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In the Early Years Foundation Stage and Key Stage 1, this teaching is supported by strong communication with parents, including resources and links shared in class and for use at home (see section 5).

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of their time at the Prep School**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Senior School:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of their time at the Senior School**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children, and those generated or altered using AI) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

- How AI tools can be used to create or alter images, video and audio, including deepfakes, and how to recognise and report manipulated content
- How to recognise misinformation, disinformation and harmful online content, including misogynistic influencer content, and where to get help

The safe use of social media and the internet will also be covered in other subjects where relevant.

Pupils will be taught about the risks associated with mobile phones, both in school and more broadly, and about the benefits of a mobile phone-free school environment, in line with the DfE's Mobile phones in schools guidance.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters and regular Online Safety updates in the weekly newsletter, A View of The Close. Online Safety videos designed for parents by an external online safety adviser are sent out every few weeks.

The school lets parents know about the systems it uses to filter and monitor online use, what pupils are being asked to do online, the sites and platforms they may be asked to access, and who from the school (if anyone) they may interact with online.

The Mobile Phone Policy, and the reasons for it, are explained to parents, who are asked to reinforce it at home. Details of the policy are published on the College website.

Parents will usually be informed and involved where an online safety concern arises involving their child, including a filtering breach, unless doing so could place a child at greater risk of harm or undermine a police or statutory safeguarding response.

Where the school becomes aware of harmful online challenges, trends or hoaxes, it will respond proportionately, giving clear advice without amplifying harmful content or causing unnecessary anxiety.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headmaster and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headmaster.

The following national organisations provide information to help support parents:

- Childnet
- Internet Matters
- NCA-CEOP
- Parent Zone

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. Please see the school's Anti-Bullying Policy and Behaviour Policies (Prep and Senior School).

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Anti-Bullying Policy and the Behaviour Policy, and the incident will be recorded on the College Bullying Log. Where the behaviour may amount to child-on-child abuse, or raises any other safeguarding concern, staff will also report it to the DSL, who will record it on My Concern and respond in line with the Safeguarding and Child Protection Policy.

Disciplinary and safeguarding action may proceed alongside one another. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Where the DSL has reasonable grounds to suspect that possessing the material is illegal, they will report the incident to the police as soon as is reasonably practicable. Staff will not copy, forward, save or print the material; devices will be secured and the police will advise on how the material is handled. Incidents involving nude or semi-nude imagery, including AI-generated imagery, will be managed in line with section 4.2 of the Safeguarding and Child Protection Policy and the UKCIS guidance. The DSL will also work with external services where it is necessary to do so.

6.3 Examining Electronic Devices

The Headmaster, and any member of staff authorised to do so by the Headmaster, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as an item for which a search may be conducted (section 4.1 of the Behaviour and Discipline Policy – Senior School includes mobile phones and other personal interactive communication devices where their possession, access or use is contrary to College rules, and section 9.1 confirms that such items may be searched for; see also section 6.2 of the Mobile Phone Policy), and/or
- Is evidence in relation to an offence

The conduct of the search itself, including seeking the pupil's cooperation, the presence of a second member of staff, recording and informing parents, is governed by section 9 of the Behaviour and Discipline Policy – Senior School (in particular 9.2, Conduct of a search, and 9.4, Records, parents and disposal), or the equivalent section of the Prep School behaviour policy. Every search is recorded, whether or not an item is found. Before carrying out a search, the authorised member of staff will assess how urgent the search is and consider the risk to other pupils and staff.

If the search is not urgent, they will:

- Seek advice from the DSL or a DDSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or DDSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image

- Not copy, print, share, forward, save or delete the image, or ask the pupil to do so
- Secure the device and report the incident to the DSL (or a DDSL) immediately. The DSL will decide what to do next in line with section 4.2 of the Safeguarding and Child Protection Policy, the DfE's guidance on searching, screening and confiscation and the UKCIS guidance on sharing nudes and semi-nudes

Any searching of pupils will be carried out in line with the DfE's latest guidance on searching, screening and confiscation.

The DSL will be informed of any search where there were reasonable grounds to suspect a pupil was in possession of a prohibited item, or where a search identifies a potential safeguarding risk, in line with section 3.1 of the Safeguarding and Child Protection Policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement (younger pupils in the Prep School do not sign themselves, and instead there is more of a discussion) regarding the acceptable use of the school's IT systems and the internet.

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.

Use of the school's devices and networks is monitored to detect safeguarding risks, in line with section 6.3 of the Safeguarding and Child Protection Policy. All users are informed that use of school devices and networks can and will be monitored, and all monitoring is carried out in line with data protection, human rights and privacy legislation.

Filtering and monitoring apply to all users, including guest accounts, on all school-owned devices and on any device using the school's internet connection. Anyone who accidentally or deliberately accesses, witnesses or suspects that unsuitable material has been accessed must turn off or lock the screen (using Jamf Teacher for pupil iPads), report the concern to the DSL, and report the URL to the IT staff where it can be identified, as set out in section 6.3.3 of the Safeguarding and Child Protection Policy.

Where pupils use their own laptops or tablets for learning, these are used in line with the Acceptable Use Policy. Mobile phones are not part of any bring your own device (BYOD) arrangement.

More information is set out in the acceptable use agreements.

8. Pupils Using Mobile Devices in School

The detailed rules, times, exceptions and sanctions for mobile phones are set out in the Mobile Phone Policy. This section summarises them and sets out the online safety and safeguarding principles that apply. Where the two differ, the Mobile Phone Policy governs

the day-to-day rules and the Safeguarding and Child Protection Policy governs any safeguarding matter.

Dover College is a mobile phone-free environment by default, in line with the DfE's statutory Mobile phones in schools guidance, section 6.2 of the Safeguarding and Child Protection Policy and section 5.1 of the Mobile Phone Policy. Pupils do not have access to mobile phones during the school day, including:

- Lessons and tutor group time
- The time between lessons, break times and lunchtime
- Clubs, activities and events organised by the school, including those before or after the school day, unless the member of staff leading the activity authorises use for a specific purpose

Prep School pupils may bring a mobile phone to school only where they travel by school bus or another travel arrangement has been agreed, and must hand it in to the Prep School office on arrival and collect it at the end of the school day (section 5.2 of the Mobile Phone Policy).

In the Senior School, pupils from Shell to Fifth Form who bring a mobile phone to school must hand it in to their House at the start of the school day. Devices are stored securely and returned before pupils depart at the end of the school day (section 5.3 of the Mobile Phone Policy).

Sixth Form pupils may keep their mobile phones during the school day, reflecting their increasing independence and responsibility. Use is permitted only in the Sixth Form Centre, or when specifically authorised by a member of staff for a lesson, educational activity, trip or visit. Phones must not be used in areas shared with younger pupils. Sixth Form pupils sign the acceptable use expectations in Appendix 1 of the Mobile Phone Policy (section 5.4).

Individual exceptions, for example for a medical condition, a disability, SEND, a safeguarding or welfare plan, or exceptional family or travel circumstances, are agreed and recorded in line with section 5.5 of the Mobile Phone Policy. An exception allows use only for the specific purpose, time and place agreed.

The mobile phone-free approach must never stop a pupil from reporting a concern. Where a pupil needs to show staff messages, images or other content as part of reporting a concern, staff will allow supervised access to the device, will avoid viewing or sharing illegal or harmful content unnecessarily (and will never view suspected nude or semi-nude imagery), and will report the concern to the DSL, in line with section 5.8 of the Mobile Phone Policy.

Any use of mobile devices in school by pupils must be in line with the Acceptable Use Policy for Pupils.

Breaches are managed under section 6 of the Mobile Phone Policy and the Behaviour and Discipline Policy – Senior School, which lists unauthorised use or possession of a mobile phone during the College day as unacceptable conduct (section 4.2). Sanctions and confiscation will be proportionate and will take account of the pupil's circumstances. Where the behaviour gives cause to suspect that a pupil is at risk of harm, staff will report it to the DSL.

Parents who need to contact their child during the school day should do so through the College office (section 8 of the Mobile Phone Policy). Arrangements for mobile phones on trips, visits and residential activities are set by the trip leader and reflected in the trip planning and risk assessment, in line with section 5.7 of the Mobile Phone Policy and the Safety & Supervision on Educational Visits Policy.

Boarding houses

During the teaching day, boarders follow the same rules as day pupils. Outside the teaching day, House arrangements apply: boarders from Shell to Fifth Form hand their phones to House staff at the agreed time before bed, and Sixth Form boarders may keep their phones overnight unless an individual welfare or safeguarding arrangement provides otherwise. The College makes arrangements for boarders to contact their families in private at a suitable time, taking account of time zones for international pupils, in line with the National Minimum Standards for Boarding Schools and section 5.6 of the Mobile Phone Policy. Any concern arising from a boarder's device use is reported in line with the Safeguarding and Child Protection Policy.

Staff, visitors and parents

Expectations for staff, volunteers, contractors, visitors and parents are set out in sections 3, 4 and 8 of the Mobile Phone Policy. In particular, staff must not use personal mobile phones for personal activity while supervising pupils, must not give personal contact details to pupils, and must not use personal devices to photograph or record pupils. Any concern arising from an adult's use of mobile technology is managed under the Safeguarding and Child Protection Policy and the Staff Code of Conduct.

9. Staff using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates
- Keeping the device protected by a strong password or passphrase, in line with the password requirements in the Staff (and Volunteer) IT Acceptable Use Policy & Agreement, and using multi-factor authentication wherever it is available
- Work devices must be used solely for work activities.

- Reporting a lost or stolen device, a suspected phishing attempt, a compromised account or any possible data breach to the Network Manager immediately, in line with section 6.4 of the Safeguarding and Child Protection Policy

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

Early Years Foundation Stage (see Appendix 3 of the Safeguarding and Child Protection Policy and section 4 of the Mobile Phone Policy):

- Staff must not use personal mobile phones, cameras or other personal devices with imaging or sharing capabilities in EYFS teaching or care areas or while supervising EYFS children; such devices are locked away during contact time. Nominated staff may carry a personal phone on outings, for emergency contact only (section 4 of the Mobile Phone Policy).
- Only school devices may be used for photographs and observations.

- Cameras, mobile phones and other devices with imaging and sharing capabilities are not permitted in toilet and nappy changing areas.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy and Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Section 4.2 of the Behaviour and Discipline Policy – Senior School identifies as unacceptable conduct: online or off-site behaviour which threatens, harms or harasses another person; creating, requesting, possessing or sharing nude or semi-nude images or AI-generated sexual images; and photographing, recording or sharing images of another person without consent. Where such conduct also raises a safeguarding concern, it is

reported to the DSL and managed under the Safeguarding and Child Protection Policy, and disciplinary and safeguarding action may proceed alongside one another.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Where a concern about a member of staff's use of technology suggests that they may have harmed a child, or may pose a risk of harm to children, it will be referred to the Headmaster (or to the Chair of Council where the concern relates to the Headmaster) and managed under section 8.2 of the Safeguarding and Child Protection Policy, including referral to the LADO where required. Concerns that do not meet that threshold are managed as low-level concerns under the low-level concerns policy and the Staff Code of Conduct.

The school will consider whether incidents which involve illegal activity or content, or are otherwise serious, should be reported to the police. Where there is an immediate risk of harm, the emergency services will be contacted on 999. Suspected child sexual abuse material will be reported in line with section 6.3.3 of the Safeguarding and Child Protection Policy, which may include the Internet Watch Foundation and NCA-CEOP.

Misuse of AI tools, including the creation or sharing of AI-generated or digitally manipulated images of pupils or staff, will be responded to in line with section 6.1 of the Safeguarding and Child Protection Policy and the AI Policy.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying, the risks of online radicalisation, the Mobile Phone Policy, and their roles and responsibilities in relation to filtering and monitoring.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages

    - Non-consensual sharing of nude and semi-nude images and/or videos (including AI-generated or digitally altered imagery), especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- AI tools can be used to create harmful content, including deepfakes and nude or semi-nude imagery of children, and any such concern is a safeguarding matter to be reported to the DSL
- Filtering and monitoring are not a standalone solution, and supervision, vigilance and prompt reporting remain essential

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive safeguarding and child protection training, including online safety, at induction, and this training will be regularly updated, in line with section 7.1 of the Safeguarding and Child Protection Policy.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in section 7 of the Safeguarding and Child Protection Policy.

12. Monitoring arrangements

Online safety concerns with a safeguarding dimension are recorded on My Concern. Routine behaviour is recorded on the school's behaviour-management system and bullying on the College Bullying Log, in line with section 7 of the Behaviour and Discipline Policy – Senior School. The same incident may need entries on more than one system.

This policy will be reviewed at least annually by the DSL and Online Safety Lead, and will be shared with the governing body at every review. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online, as set out in section 6.9 of the Safeguarding and Child Protection Policy. This is important because

technology, and the risks and harms related to it, evolve and change rapidly. The policy will be reviewed sooner following a significant online safety incident, a change in technology or working practice, or a change in national or local guidance.

The school's filtering and monitoring provision is reviewed at least once every academic year, and system checks are carried out and recorded termly, in line with section 6.3.2 of the Safeguarding and Child Protection Policy.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour and Discipline Policy – Senior School, and the Prep School behaviour policy
- Anti-Bullying Policy
- Mobile Phone Policy
- Staff Code of Conduct
- GDPR Policy and Privacy Notices
- Complaints Procedure
- Acceptable Use Policy (Pupils and Staff)
- RSE Policy
- Social Media Policy
- AI Policy
- Use of Mobile Phones and Digital Photography Policy in EYFS (Appendix 3 of the Safeguarding and Child Protection Policy)

- Safety & Supervision on Educational Visits Policy
- Low-level Concerns Policy