Online Safety Policy

CATERHAM SCHOOL

CATERHAM PREP

Policy Authors:	Louise Fahey (Assistant Head Pastoral and DSL)
Date Reviewed By Authors:	September 2025 with Senior Deputy Head, Deputy Head (Prep) and Head of the Pre-Prep
Next Review Due:	September 2026

Introduction

The School prides itself on its innovative approach to the use of technology in line with its ethos and aims and is recognised as a leader in this field. As an Apple Distinguished School, a TES Independent Schools Award winner for 'best use of technology' we continue to explore the educational opportunities afforded by the use of technology. As we embrace innovation and technology, safeguarding remains at the heart of every decision.

This Online Safety Policy empowers us to protect and educate pupils, and staff, in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

All staff and pupils from Prep Year 3 to 5th Year Senior School are given an iPad to support and enhance their learning, whilst younger pupils benefit from shared iPad use. This is supported by a powerful infrastructure including excellent Wi-Fi, cloud storage and Apple TV in every classroom.

The use of these exciting and innovative tools in school and at home has been shown to raise attainment and support learning, however, the unrestricted use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face are included in KCSIE 2025:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users; 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: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce - risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies:

- Safeguarding policy
- Anti-Bullying policy
- Behaviour Policy
- Wellbeing Policy
- Staff Code of Conduct
- EDI Policy
- Searching a Pupil Policy
- Staff Acceptable Use Policy (Appendix A)
- Pupil Acceptable Use Policies (Senior School) (Appendix B & C)
- Pupil Acceptable Use Policy (Prep School) (Appendix D)
- Pre-Prep Virtual School Acceptable Use Agreement (Appendix E)
- Staff Social Media Policy (Appendix F)
- Pupil Social Media Policy (Appendix G)

- Online Safety Expectations (Appendix H)
- Laptop Acceptable Use Policy (Appendix I)
- AI policy (Appendix J)

Underpinning the following Online Safety Policy are the frameworks and Government legislation set out in:

- Keeping children safe in Education (2025)
- Working together to Safeguard Children (2018, updated Dec 2023)
- Meeting Digital and Technology Standards in Schools and Colleges' (DfE, 2023)
- Sharing of nudes and semi-nudes: advice for education settings working with children and young people (DfE 2020, updated March 2024)
- Generative artificial intelligence (AI) in education (DfE, June 2025)
- The Online Safety Act (July 2025) In June 2025, the DfE published detailed guidance and policy papers outlining expectations and best practices for the safe and effective use of AI in education settings.
- NMS 2022

All staff are expected to be familiar with the DfE guidance and processes outlined in the School's safeguarding policy. This policy explains how we intend to manage potential risks, while also addressing wider educational issues to help our pupils (and their parents) to be responsible users and stay safe while using the internet and other communications technologies.

Leadership of Online Safety

The DSL takes responsibility for online safety within the school. The Trustee with responsibility for online safety is Deborah Grimason. The DSL liaises closely with the Senior Deputy Head, Deputy Head (Innovation), Director of IT Services and the Head of Wellbeing to look at any aspects of online safety that need to be addressed.

The DSL will:

• Act as main point of contact on online safety issues and liaise with other members of staff as appropriate.

• Ensure policies and procedures that incorporate online safety concerns are in place. This should include but is not limited to; Safeguarding policy; Acceptable Use Policies (AUPs), mobile phones, child on child abuse (including responses to cyberbullying and sexting/youth produced imagery), and filtering and monitoring.

• Ensure there are robust reporting pathways (CHIP/ OurCaterham) and signposting to internal, local and national support.

• Record online safety incidents and actions taken. Review any reported online safety incidents to inform and improve future areas of teaching, training and policy development

• Ensure the whole school community is aware of what is safe and appropriate online behaviour and understand the sanctions for misuse.

• Liaise with the local authority and other local and national bodies as appropriate.

• Work with the Director of IT Services to ensure that appropriate filtering and monitoring is in place and that the DfE standards for filtering and monitoring are being met.

• Take appropriate action in line with child protection policies and procedures, if the filtering system and monitoring approaches identify any causes for concern.

• Implement regular online safety training for all members of staff (including as part of induction) that is integrated, aligned and considered part of the overarching safeguarding approach (KCSIE 2025).

• Work with staff to ensure that appropriate online safety education is embedded throughout the curriculum; promoting the responsible use of technology and empowering children to keep themselves and others safe online.

• Actively engage with local and national events to promote positive online behaviour, e.g. Safer Internet Day and anti-bullying week.

• Update the school's online safety risk assessment on an annual basis in conjunction with the Director of IT Services and Deputy Head (Innovation)

• Ensure that online safety is promoted to parents and carers and the wider community through The Wellbeing Hub (Senior School), Tooled Up Education (Prep School). parent webinars and the School newsletter.

• Ensure that their own knowledge and skill are refreshed at regular intervals to enable them to keep up to date with current research, legislation and trends. To understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school; can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online.

• Feedback online safety issues to the senior management team and other agencies, where appropriate, including Children's Social Care and the LADO

• The DSL will follow the guidance around harmful online challenges and online hoaxes when supporting children and sharing information with parents/carers.

The DSL should be aware of the potential for serious child protection issues to arise from online safety issues, including:

• Sharing of personal data

• Access to illegal / inappropriate materials

• Inappropriate on-line contact with adults / strangers

• Potential or actual incidents of grooming and/ or extortion

• Online bullying

Pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the DSL will consider a referral into the Cyber Choices programme.
This programme aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

The Director of IT Services

The Director of IT Services is responsible for ensuring:

• That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

• That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.

• The school's filtering policy is applied, reviewed and updated on a regular basis.

• That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

• That the use of the network / digital platforms / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the appropriate staff for investigation / action / sanction.

• That monitoring software / systems are implemented and updated as agreed in school policies.

• That secure and effective remote working systems and expectations are in place for staff and that guidelines are updated and distributed as required.

• That they liaise with the DSL to effectively safeguard pupils online within school and at home.

Teaching Staff

Teaching staff are responsible for ensuring that:

• They have an up-to-date awareness of online safety matters, current security threats and of the current school online safety policy and practices including an understanding of the filtering and monitoring processes in place.

• They have read and understood the school Staff Acceptable Use Policy (AUP) and the online safety policy.

• They act on any suspected misuse or problems (for example failure to comply with the conditions of the AUP), recording incidents and action on CHIP. More serious concerns should be reported to a member of the safeguarding team or the pupil's Head of Year for investigation / action / sanction.

• Digital communications with pupils (email / Teams / etc.) should be on a professional level and only via official school systems.

• Online safety issues are embedded in all aspects of the curriculum and other school activities.

• Pupils understand and follow the school Online Safety Rules displayed in all classrooms and the Pupil Acceptable Use Policy.

• Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. Teachers should ensure that pupils only use AI to enhance and develop their work when permitted, using school approved AI tools (Rileybot) and that pupils are transparent about this when work is submitted.

• They monitor ICT activity in lessons, extra-curricular and extended school activities, recognising that a pupil's personal devices may bypass the school's filtering and monitoring systems.

• They are aware of online safety issues related to the use of mobile phones, cameras, wearable technology and handheld devices and that they monitor their use and implement current school policies with regard to these devices.

• In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

• They celebrate the positive use of ICT and digital media and promote correct usage.

Pupils

• Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they accept before being given access to school systems.

• Understand the need to avoid plagiarism and uphold copyright regulations. Pupils only use AI to enhance and develop their work when specifically permitted by their teachers, using school approved AI tools (Rileybot) and should be transparent about this when work is submitted.

• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• Will be expected to know and understand school policies on the use of mobile phones and smart devices. They should know and understand school policies on the taking / use of images and on cyber-bullying.

• Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if members of the school community or learning is impacted in any way.

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will ask all new parents to sign the parent /pupil agreement when they register their child with the School, which includes agreed use of technology. The school will support parents by providing access to resources and webinars via The Wellbeing Hub (Senior School), Tooled Up Education (Prep School) delivering school-led webinars and ensuring parents are aware of national campaigns, support organisations and current online safety issues. Parents are provided with information about the filtering and monitoring systems on School iPads and advised that parental controls should be applied to personal devices.

• Parents are strongly encouraged to engage with the online safety resources on The Wellbeing Hub (Senior School parents) or Tooled Up Education (Prep parents) and attend the parent webinar in the Autumn term.

Teaching and learning

The internet and other digital technologies are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. As well as encouraging creativity, stimulating discussion. affording excellent research opportunities, it also enables the sharing and review of work through our Apple TV mirroring system, flipped learning opportunities, innovative ways of submitting and of marking work, as well as disseminating notes and information. Beyond this, and perhaps more importantly, the routine use of iPads and technology prepares pupils for a world which is increasingly dependent on digital technologies.

Online Safety education will be provided in the following ways:

- In the senior school dedicated time in Wellbeing lessons or tutor sessions at the start of the school year supports pupil engagement with our expectations. An individual declaration of understanding and agreement is confirmed through a short online quiz.
- A planned online safety programme is provided as part of the Wellbeing curriculum. In addition to this key online safety messages will be reinforced to each year group through assemblies, tutor time and whole school initiatives.
- Online Safety resources and support pathways are available to staff, pupils and parents through The Wellbeing Hub (Senior School) and Tooled Up Education (Prep School).
- Pupil should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of technology, the internet and smart devices both within and outside school. They should also be educated about protecting their own devices (such as password protecting their mobile and tablets) and not sharing passwords or personal information.
- Staff should act as good role models in their use of technology, the internet and smart devices.
- ***Online safety expectations*** will be posted in all classrooms.
- Pupils are routinely informed that network and internet use will be monitored.

Important Information for pupils about School Devices and Use of Devices on School Premises

iPads

Pupils with school-distributed iPads must adhere to and sign the ***Pupil Acceptable Use Policy*** with the understanding that the school reserves the right to reclaim the iPad at any time and that it remains the property of the school at all times.

Please Note:

The iPads are covered by insurance for accidental damage and theft. If a device is damaged it should be reported to the IT Workshop immediately (pupils should email ITsupport@caterhamschool.co.uk in the first instance, explaining what happened to the

device, when and where). Pupils will then fill out an accident report form and the device will be sent to the insurance company who will decide if the claim is valid. Pupils who make more than one insurance claim a year will be charged £50 for each subsequent claim.

If the device is stolen, it must be reported to the Police within 24 hours and a crime reference number obtained. Failure to do this in a timely manner will result in the claim being dismissed. Similarly, the device must have been secured at the point of theft for the claim to be valid.
If the insurance company rejects a claim, the cost of a replacement device will be added to the following term's bill.

Please also note that iPad cases are not insured, but are a prerequisite for the insurance to be valid. All iPads must be kept in the assigned case at all times. If the case is damaged through a user fault, the cost of a replacement will be added to the following term's bill. Pupils must replace lost cables or plugs, but must purchase Apple branded products; it is not acceptable to buy cheaper 'unbranded' replacements.

Boarders

Boarding pupils are expected to adhere to the rules within this policy during their time at the school. Where exceptions or changes are made to the above, or to the specific level of filtering being provided to individual users or boarding pupils as a whole, pupils will be notified through the boarding staff or via email.

Any problems boarding pupils have with their internet access or use of IT equipment should be reported to the IT support team.

Making sure our boarding pupils are safe online and not accessing or exposed to inappropriate material is essential. While our web filters have a significant role to play here, this alone does not prevent the possibility of boarders using mobile data to access inappropriate content, nor from their bringing inappropriate content to school already downloaded onto a device. In caring for our boarders, the School seeks to balance our duty of care to keep them safe with their rights to privacy and a homely environment. We adopt a profiled approach to mobile devices, which sees pupils up to 4th Year inclusive hand their devices in at bedtime, while our 5th Year and Sixth Form pupils are trusted to hold theirs and behave responsibly. However, any online/mobile phone concerns about individual pupils in these older years sees their devices handed in for an appropriate period of time. We promote (as indeed we do with all pupils) **a culture of courageous reporting** if they are aware of inappropriate content on a device, and ally this with assemblies and Wellbeing lessons which highlight the importance of making responsible choices online. If we have suspicions about a boarder accessing or possessing inappropriate material, we follow the protocols set out in our relevant policies (listed above).

BYOD

Bring Your Own Device (BYOD) is only available to those in the Sixth Form.

Pupils in the Sixth Form are expected to have agreed to the BYOD version of the Pupil Acceptable Use Policy. Any questions about this should be raised with the tutor or Head of Year who will pass them on to the relevant member of staff.

WHAT YOU NEED TO KNOW:

- Personally-owned devices are never to be plugged into the wired network.
- Devices should use the 'caterham wifi' network
- You may find that Wi-Fi coverage is limited in some parts of the school

- Device usage is solely for educational purposes
- Pupils must get approval from a teacher before getting a device out in class
- The only permissible devices for use in the classroom are an iPad or Apple MacBook. Phones are not an acceptable alternative.

Personal Information, Data Protection and Your Safety Online:

Personal details include your name, date of birth, telephone number, email address, where you live and where you go to school. Whilst it is not always possible to avoid entering some of this information, you should consider the following:

- Where possible usernames should be anonymous, and your name may be entered as First Name followed by your First Initial.
- Wherever possible, the email address given should always be the anonymised version of your school email address. Never use a personal email address when signing up for a school-endorsed program.
- Consider carefully whether or not the service you are signing up for is 'safe' and if you are happy for this company to have information about you stored on file.

Virtual Learning Protocols & Safeguarding

In response to working practices which have emerged since Covid, all parents are asked to give consent for teachers and pupils to meet virtually 1-to-1 to participate in academic or co-curricular activities. The wording below outlines the terms of the agreement and is in line with our broader safeguarding policy:

During timetabled lessons and indeed online clubs, activities and clinics, it is possible that a situation will arise where there is only one pupil and the teacher in the virtual meeting. There are statutory safeguarding implications when we are working one-to-one with pupils and, as a consequence, we require formal parental permission to proceed along these lines should the situation arise. (One-to-one meetings that fall outside of these parameters will follow our previously published protocols by which a teacher will contact you directly to seek consent and agree a time to contact your child)

Managing Internet Access

Information system security is of paramount importance to the School. Our IT system security is reviewed regularly and virus protection will be updated regularly. Security strategies derive from national and local authority guidelines.

E-mail and Communication

Pupils and staff may only use approved e-mail accounts and learning platforms (Microsoft Teams) on the school system.

Pupils and staff should immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. The email should not be responded to.

Staff to pupil email communication must only take place via a school email address or from within the learning platforms and will be monitored.

Unsolicited incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. The forwarding of chain letters is not permitted.

• Any digital communication between staff and students or parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

Incident Management Procedures

Caterham School will take all reasonable precautions to ensure online safety for all staff and pupils but recognises that incidents may occur within and outside of school which will need intervention. We will ensure:

• there are clear reporting pathways which are understood and followed by all members of our school community.

• reports will be dealt with as soon as is practically possible once they are received

• the Pastoral Leadership Team, Safeguarding Team and other responsible staff have appropriate skills and training to deal with online safety risks.

• If staff are concerned that an incident involves any illegal activity or the potential for serious harm, they should refer to the detailed guidance in the School's Safeguarding Policy and contact the DSL who will follow guidance set out in KCSIE 2025 and, if appropriate, the UK Council for Internet Safety's 'Sharing nudes and semi-nudes' which can be found here. Under no circumstances should concerns be investigated or content on devices be viewed.

This may include:
o Non-consensual images/ Self-generated images
o Child on child abuse
o Terrorism/extremism
o Hate crime/ Abuse
o Fraud and extortion
o Harassment/stalking
o Child Sexual Abuse Material (CSAM)
o Child Sexual Exploitation Grooming
o Pornography
o Sale of illegal materials/substances
o Cyber or hacking offences under the Computer Misuse Act
o Copyright theft or piracy

• any concern about staff misuse will be reported to the Headmaster, unless the concern involves the Headmaster, in which case the complaint is referred to the Chair of Trustees.

• incidents involving pupils should be logged on CHIP.

• relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g., local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.

• where possible those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)

Published content and the school website

The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information are not published.) The Director of Marketing takes overall editorial responsibility and ensures that content is accurate and appropriate.

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school generally seeks to use group photographs rather than full-face photos of individual children, although there are exceptions. Pupils' full names will be avoided on the website and other social media. Permission is sought in line with our general Privacy Notice which can be found on the school website, updated recently to be GDPR compliant.

• Staff are allowed to take digital / video images to support educational aims, but must follow school safeguarding policy concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment, the personal equipment of staff should not be used for such purposes.

• Pupils must not take, create, use, share, publish or distribute images of other pupils without their permission. It must be recognised by pupils that these permissions can change depending on the relationship between particular groups of students.

Social networking and personal publishing

The School's policy on social networking is robust:

The School controls access to social networking sites, and considers how to educate pupils in their safe use, such as the use of passwords, private groups and the publishing of personal or sensitive information through the school's Wellbeing curriculum and the support offered by tutors. This control may not mean simply blocking every site, which is usually counter-productive; it is often more effective and valuable to monitor and educate pupils in their use.

Pupils are advised never to give out personal details of any kind which may identify them or their location. Further guidance on this matter is explored in the pupil ***Acceptable Use Policy*** and the pupil ***Social Media Policy*** found in the appendix of this document. Pupils are educated about the benefits and risks of the internet and social media through the Wellbeing curriculum, details of which can be found in the school's ***Wellbeing Policy***. This guidance is informed by the School's own experiences with social media and by Keeping Children Safe in Education 2025 and its relevant additional documentation.

Filtering and Monitoring

Caterham School takes all reasonable steps to safeguard pupils online through appropriate Filtering and Monitoring systems, following the guidance in Filtering and Monitoring Standards for Schools and Colleges (2023) which can be found here.

The DSL will work closely with the Senior Leadership Team, Director of IT Services and named Trustee to ensure that systems are robust, effective and reviewed according to the

guidance. Outcomes are recorded and inform reviews of the Safeguarding Policy, Online Safety policies, training, curriculum opportunities, procurement decisions and monitoring strategies.

Smoothwall monitoring is applied to all School iPads, restricting access to inappropriate or harmful content or websites, whether a pupil is onsite or offsite. Between the hours of 8am – 6pm Monday to Friday (term time only) the safeguarding team will be notified of any concerns by email via an alert system.

The filtering and monitoring policies continue to operate on iPads 24/7, any further concerns are recorded in a report accessed by the DSL the following school day. The School will only be aware of concerns during school opening hours.

The report highlights any concern relating to online activity which reaches a safeguarding threshold. This report allows the DSL to explore potential patterns and risks in a timely manner in line with our safeguarding duties, including the PREVENT duty. A record of concerns and outcomes is maintained by the DSL.

For Sixth Form pupils who bring their own devices to school, filtering and monitoring will occur whilst on the school site and the device is connected to the school's internet.
No pupil will be permitted to use a VPN allowing them to bypass our monitoring systems and leaving them unprotected.

All staff have a duty to support the School's Filtering and Monitoring responsibilities. The following concerns should be reported to the DSL:

- Witnessing or suspecting unsuitable material has been accessed
- Being able to access unsuitable material
- Teaching activities which could create unusual activity on the filtering logs
- Being aware of a failure or abuse of the system
  Noticing abbreviations or misspellings that allow access to restricted material

Emerging Technologies and AI

The use of technology, including AI-enabled software, is an integral part of education in the 21st century. Any emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Our school is committed to promoting responsible and ethical use of these resources to ensure that emerging technology is used in a way that benefits our community and promotes learning and growth. The use of AI-enabled software is permitted in accordance with agreed guidelines (see Appendix J).
All pupils have access to Rileybot, the school approved AI tool, and are permitted to use this to enhance and develop their work when specifically permitted by a teacher.

Mobile Phones and Smart Devices

Caterham School has a clear and structured approach to the use of mobile phones, tailored to different parts of the school. This approach ensures a focused learning environment, whilst recognising the benefits of technology when used in age-appropriate ways.

Prep School

Within the Prep School (Years 1-6) mobile phones are not permitted during the school day.

• If a pupil needs to bring a phone to school (for instance, if they travel by bus), they must hand it in at Reception upon arrival.

• Phones are securely stored and can be collected at the end of the school day.

Senior School

First Year to Fourth Years

• Pupils are provided with iPads, allowing them to access technology throughout the school day; as such there is no need for them to use phones around the school site during the school day.

• Mobile phones should be kept in lockers throughout the school day.

• If a pupil is seen using their phone during the school day, it will be confiscated and may be collected at the end of the school day from their Head of Year. For the following week, those who have used their device inappropriately will surrender it to their Head of Year each day.

Fifth Year and Sixth Form

• Pupils are permitted to use their phones during break and lunchtimes, but only in their designated year areas. This is consistent with teaching our pupils when and how to use technology positively.

• Phones are not allowed in lessons or common areas including the refectory.

Boarders

• Boarders may use their mobile phones to connect with family and friends when in the boarding houses but are required to hand in their devices at a set time each evening.

• There are designated 'device-free' times at weekends to encourage balance, wellbeing, and face-to-face connection.

• Mobile phones are not permitted in the refectory.

Wearable Technology

To minimize distractions and maintain a focused learning environment, our policy now extends to wearable technology, including but not limited to smartwatches, fitness trackers with communication features, and other internet-enabled wearable devices.

• Prep School: Pupils are not permitted to bring wearable technology to school. If a pupil must bring one (e.g., for travel), it should be handed in at Reception upon arrival and collected at the end of the day.

All communication between parents and children during school hours should go through the school office to maintain proper supervision and security.

• First Year to Fourth Years:

As pupils are equipped with iPads for technology needs during the school day, wearable technology should be kept in lockers or, if worn, should remain in flight mode (or an equivalent disconnected state) throughout the school day.

Any wearable device found connected or in use during the day will be confiscated and returned at the end of the school day. Any wearable device seen in use with social media or personal emails during the day will be confiscated and returned at the end of the school day.

• Fifth Year and Sixth Form: Wearable technology may be used during break and lunchtimes, but only within designated year areas

Staff will use a school phone where contact with pupils is required.

Managing videoconferencing

Pupils should ask permission from the supervising teacher before making or answering a videoconference call (Teams, for instance).

Videoconferencing will be appropriately supervised for the pupil's age.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to GDPR compliance.

Staff should ensure that confidential, personal data is not stored on personal devices.

Staff and the Online Safety Policy

All staff will be given the School's ***Online Safety Policy***, and related policies and procedures, and their importance explained. All staff will sign the annual safeguarding declaration acknowledging that they have read and understood the Online Safety Policy and agree to work within the agreed guidelines. Staff are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT use will be supervised by the DSLs and have clear procedures for reporting issues.

Appendix A

IT Acceptable Use Policy for Staff and Trustees

IT and related technologies such as email, the internet and mobile devices are integral to our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. Any concerns or clarification should be discussed with the DSL, Director of IT Services or Senior Deputy Head.

As a member of staff or trustee, you are required to adhere to the following statements:

- I understand IT includes all devices and platforms (school and personal when used for school).
- I will only use school IT systems for authorised purposes and that misuse may be a criminal offence.
- I will only use the school's email, internet, learning platforms and related technologies for professional purposes, or for uses deemed 'reasonable' by the Headmaster or Board of Trustees.
- I will keep my passwords secure and understand that I am responsible for all activity under my username.
- I will use only the school's approved, secure email system for school business.
  I will keep personal/sensitive data secure, use it appropriately, whether in school, taken off the school premises or accessed remotely. Sensitive personal data should not be transferred to external hard drives, including USB sticks.
- I will follow the school's Remote Working Guidance when off-site.
- I will follow the school's AI Policy and will ensure any AI-enabled tool or platform used with pupils is age-appropriate, compliant, and used transparently. I will not enter identifiable or sensitive information into public AI platforms.
- I will comply with GDPR, the Privacy Notice, and data retention policies and will request guidance from the school Data Protection Officer if I am unsure.
- I will not install hardware or software without the permission of the Director of IT Services.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I accept that my internet/email use on school networks/devices may be monitored.
- I understand that the School's Filtering and Monitoring systems constantly assess online activity and operate on and offsite and that concerns will be recorded and followed up as appropriate.
- I understand my role in supporting the School's Filtering and Monitoring responsibilities to safeguard pupils
- I will respect copyright and intellectual property rights.
- Images and recordings of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent or staff member. Images and recordings will not be distributed outside the school networks without the permission of the parent, member of staff or Headmaster.
- I will ensure my online activity does not bring the school into disrepute.
- I will comply with the Staff Social Media Policy.
- I will maintain professionalism in all communications with parents, pupils, and staff and strive to ensure that messages cannot be misunderstood or misinterpreted.
- All EYFS staff will ensure that personal mobile devices, including mobile phones and cameras, are kept out of sight and reach of pupils.

- I will support the school's Online Safety Policy and help pupils to be safe and responsible in their use of IT and related technologies.
- I will follow safeguarding protocols for video conferencing, especially 1:1 meetings.
- I will report safeguarding concerns to the DSLs or Headmaster immediately.
- I understand that sanctions for disregarding this policy will be in line with the School's disciplinary procedures and serious infringements may be referred to the police.

Accompanying documents to read:

- Online Safety Policy
- Staff Social Media Policy
- Pupil Acceptable Use Policy
- AI Policy

Appendix B

Caterham School – Pupil IT Acceptable Use Policy (1st–5th Year)

As a member of the Caterham School community, your use of technology should be respectful, responsible, and safe - reflecting positively on yourself and the school.

Your online presence (digital footprint) should be a positive one, as should your use of technology in school.

General Use

- I understand that the school owns the IT systems and sets rules for their use. Misuse may be a criminal offence.
- I will only use School devices and systems as directed by my teachers.
- I will never use online platforms to bully, harass, or offend others
- I will take responsibility for my online presence and ensure I do not bring the school into disrepute.
- I understand that online games are not permitted during the school day.
- I will ensure that my phones and/or smart devices are not be visible in classrooms and common areas during the school day.

Online Behaviour

- I will not post, share, or view content that is offensive, violent, racist, sexist, or explicit.
- I will not send anonymous or chain messages.
- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or locations and will tell an adult should someone request these details.
- I will not take, create or distribute any images or videos of people without the consent of my teacher or without their explicit consent.
- I will not contact others via video or audio unless for schoolwork and with teacher permission.
- I will not record any lessons (in-person or virtual) without the explicit consent of my teacher.
- I will not use obscene or offensive language or view/ share inappropriate content. This includes material that is violent, racist, sexist or adult in nature.
- I understand the behaviour expected when meeting with teachers and pupils virtually for the purposes of learning

Email, Accounts & Privacy

- I will only use my school email for school purposes and where appropriate, I will use the alias email address I have been given.
- I will keep my login information private and change my password regularly. I understand I am responsible for all online activity under my name.
- I will not share or use anyone else's login.
- I will remain signed into my school-given iCloud account (ending @appleid.caterhamschool.co.uk) at all times.
- I will not connect my personal devices to the school network without permission.

Security & Monitoring

- I understand school systems are monitored both on and offsite.
- I will only be connected to the 'Caterham Wifi' network.
- I will not attempt to bypass filters or monitoring (e.g. VPNs, proxies, mobile data).
- I will not modify school equipment or install unauthorised software.
- I understand that the School's Filtering and Monitoring systems constantly assesses my online activity. I understand that the School's Filtering and Monitoring software on my School-owned device operates on and offsite and that concerns will be recorded and followed up as appropriate.

Copyright and Generative AI

- I will respect the laws of copyright and ensure that sources used are referenced.
- I will only use AI to enhance and develop my work when specifically permitted by my teacher, using school approved AI tools and will be transparent about this when work is submitted.

Online Platforms & Social Media

- I will ensure my School account profiles is my anonymised email; no personal images/ photos or names.
- I will only use Microsoft Teams features (e.g. Chat) when required for work.
- I will follow behaviour expectations for all virtual learning sessions.
- I understand that social media use is only allowed at the discretion of the teacher and the Senior Management Team.

Safeguarding

- I understand that creating, taking, sharing, sending and saving nude/semi-nude images of anyone under 18, including of myself, is illegal. I will report any attempts to access or share such content immediately.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher or parent.
- I understand that viewing/reading/modifying/storing/editing any internet traffic, or any other attempts to retrieve personal data that has been stored digitally is totally unacceptable.

Final Agreements

- I will follow these rules in and out of school while using my device.
- I have read and understood the school's Online Safety policy.
- I acknowledge and follow the Online Safety Expectations displayed in classrooms.
- I understand that by completing the annual Online Safety quiz I agree to the terms of this document.

Appendix C

Caterham School – Pupil IT Acceptable Use Policy (*6th Form BYOD*)

As a member of the Caterham School community, your use of technology should be respectful, responsible, and safe - reflecting positively on yourself and the school.
Your online presence (digital footprint) should be a positive one, as should your use of technology in school.

General Notes and Device Use

- I understand that whilst I am providing my own device for use at school, this device is still subject to a range of conditions as set out below and breaching these may result in sanctions including the removal of Wi-Fi privileges.
- I understand that the only permissible devices for use in the classroom are an iPad or Apple Macbook of any specification. Mobile Phones are not an acceptable alternative.
- I will ensure my device is signed into **OneDrive** and my school email account at all times.
- I will ensure I have a device in place to access to **OneNote** and all required learning platforms.
- I will only connect only to **Caterham Wi-Fi** whilst on the school site
- The school owns the IT systems and the Wi-Fi network and sets rules for their use. Misuse may be a criminal offence.
- I will take responsibility for my online presence and ensure I do not bring the school into disrepute.
- Phones and smart devices should not be visible or disrupt learning in classrooms or common areas during the school day.

Email, Accounts & Privacy

- I will only use my school email for school purposes and where appropriate, I will use the alias email address I have been given.
- I will keep my login information private and change my password regularly. I understand I am responsible for all online activity under my name.
- I will not share or use anyone else's login.

Online Conduct

- I will not post, share, or view content that is offensive, violent, racist, sexist, explicit or discriminatory.
- I will not send anonymous or chain messages.
- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or locations and will tell an adult should someone request these details.
- I will choose usernames that are appropriate.
- I will never use my device to bully or upset anyone and will report any instances of bullying that I come across.
- I will not do, write, or publish anything using my internet-enabled device that I would not be prepared to show to my parents, the headmaster or a future employer.
- I will not take, create or distribute any images or videos of people without the consent of my teacher or without their explicit consent.
- I will not contact others via video or audio unless for schoolwork and with teacher permission.
- I will not record any lessons (in-person or virtual) without the explicit consent of my teacher.

- I will not use obscene or offensive language or view/ share inappropriate content. This includes material that is violent, racist, sexist or adult in nature.
- I understand the behaviour expected when meeting with teachers and pupils virtually for the purposes of learning.

Security & Monitoring

- I will not attempt to bypass the School's Filtering and Monitoring systems in any way, including, but not limited to using a 3/4/5G connection, including tethering the device to my phone, nor by using a proxy server, or VPN. Nor will I adjust or alter any profiles, software or hardware, including jailbreaking the device.
- I will not modify school equipment or install unauthorised software.
- I understand that torrenting, peer to peer networks or illegal file sharing are not permitted
- I understand that the School's Filtering and Monitoring systems constantly assesses my online activity whilst on the school site.

Safeguarding

- I will not share passwords, personal details, photos, or your location.
- I understand that creating, taking, sharing, sending and saving nude/semi-nude images of anyone under 18, including of myself, is illegal. I will report any attempts to access or share such content immediately.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher or parent.
- I understand that my digital profiles for school accounts must use anonymised emails, no real photos, and minimal personal information.
- I understand that viewing/reading/modifying/storing/editing any internet traffic, or any other attempts to retrieve personal data that has been stored digitally is totally unacceptable.

Copyright and Generative AI

- I will respect the laws of copyright and ensure that sources used are referenced.
- I will only use AI to enhance and develop my work when specifically permitted by my teacher, using school approved AI tools and will be transparent about this when work is submitted.

Online Platforms & Social Media

- I will only use Microsoft Teams features (e.g. Chat) when required for work.
- I will follow behaviour expectations for all virtual learning sessions, joining and leaving meetings at scheduled times.
- I understand that social media use is only allowed at the discretion of the teacher and the Senior Management Team.

Final Agreements

- I will follow these rules in and out of school for as long as the device is being brought into the school environment.
- I have read and understood the school's Online Safety policy and the understand the guidance within ***'Important Information about your use of ICT'.***
- I acknowledge and follow the Online Safety Expectations displayed in classrooms.
- I have read and understood the school's sanctions policy for device misuse.
- I understand that by completing the annual Online Safety quiz I agree to the terms of this document.

Appendix D

CATERHAM PREP

IT Acceptable Use Agreement for Pupils – Caterham Prep School

As a member of the Caterham School community, your use of technology and the internet should show an awareness and respect for both yourself and others. Every time you use technology, or connect to the internet, you need to be aware of the possibilities that are available to you, how to behave responsibly and how to stay safe. It is important that your actions show respect to anyone that could see your presence online, whether they are directly known to you or not, now or in the future. Equally, you must ensure that you limit your audience only to those that you want to view your content wherever possible.

Your online presence (digital footprint) should be a positive one, as should your use of technology in school.

In the school, our key rules for staying safe online are:

1. **Be careful**
2. **Be kind**
3. **Tell someone**

Whenever I am online, whether at home or school, the following rules apply:

- All my online actions, especially on school platforms or when using school IDs (usernames, email addresses, etc.), should be responsible and respectful.
- The school-issued iPad is school property; I must follow set rules everywhere.
- I will ask a teacher or another adult and must have approval before using any apps or websites.
- I will not use personal electronic devices unless this has been authorised by the school in special circumstances.
- Only my school email, logins and passwords will be used. I will not share or use anybody else's.
- For Microsoft Teams, chatting and calls are reserved for school tasks. I will not have any chats that do not include a teacher.
- All communication between school and home must go through my teacher or the school office.
- One-to-one audio or video conversations are restricted and require parental and teacher agreement.
- My passwords, photos, personal details or location will remain confidential. I will notify an adult if someone requests such information.
- Everything I view, write, or send will be appropriate and not harmful. I will not view, create, or share violent, racist, sexist, homophobic, transphobic, ableist, age-inappropriate or otherwise discriminatory content.
- I will use polite language in all online interactions and notify an adult immediately if I observe unkindness or bullying.
- Recording video, audio or taking photos requires teacher permission.
- I will report any inappropriate tech use to a teacher because this will help to keep everyone safer.
- The school uses special tools to help keep us safe online (called filtering and monitoring). I will not try to get around these tools and I will tell a teacher if I see something that shouldn't be allowed or if I notice any problems with these systems.
- If I see or am sent anything online that looks fake, suspicious, or like it might be a trick (misinformation, disinformation, or conspiracy theory), I will talk to an adult and not share it.
- If I see or receive any images or videos that look strange, changed or seem like they might not be real (for example, edited or deepfake images), I will tell an adult immediately.
- I understand that if I do not behave appropriately, the school may not allow me to use the computer and/or iPad and my parents may be contacted.

Generative AI Use:

- I will only use generative AI tools under adult supervision.
- I will not share personal information about myself or others when using generative AI.
- When engaging with AI, I will avoid inappropriate inputs and will notify an adult if unsure.
- I will only use generative AI to enhance my own work, not replace it and I will be honest about how I have used it.

General Safety:

- If anything on screen worries me, I will inform an adult.
- I will seek adult guidance if unsure about something.
- I will not share pictures or personal information with anyone without teacher permission.

- I will be aware of online scams, phishing attempts and fake websites. If I am unsure, I will ask an adult before clicking on links or sharing information online.
-

Please keep this page for your reference

IT Acceptable Use Agreement for Pupils (Prep School)

The range of issues that fall within online safety is broad and continues to evolve. These risks are grouped into four main categories, as outlined in Keeping Children Safe in Education (KCSIE) 2025:

- **Content**: Exposure to illegal, inappropriate, or harmful material, such as pornography, self-harm or suicide content, extremism, racism, misogyny, misandry, anti-Semitism, and radicalisation. KCSIE 2025 now explicitly includes **misinformation, disinformation (fake news), and conspiracy theories** as risks in this category. This also includes **AI-generated deepfake or exploitative images involving pupils**, which are an emerging form of online harm.
- **Contact**: Harmful online interactions with others, including peer pressure, commercial advertising, and adults posing as children or young people to groom or exploit for sexual, criminal, financial or other purposes.
- **Conduct**: Online behaviour by pupils themselves that increases the likelihood of, or causes, harm. This includes making, sending, or receiving explicit images (such as consensual and non-consensual sharing of nudes or semi-nudes and/or pornography), sharing other explicit images, and online bullying. This also includes engaging in or being targeted by **AI-enabled manipulation or exploitation**.
- **Commerce**: Risks related to online gambling, inappropriate advertising, phishing, financial scams, and manipulative commercial activity.
- To address these risks, the school maintains robust **filtering and monitoring systems** in line with Department for Education (DfE) guidance. We educate pupils and staff and parents (for example through workshops) about the evolving nature of online risk, including those posed by generative AI tools, and we have clear protocols for responding to all incidents, including those involving AI-generated content or deepfake imagery.

Parents, once you have read the Acceptable Use Agreement and discussed it with your child(ren), please
complete the form below (or click the link or scan the QR code if it does not display automatically) to complete a Microsoft Form to acknowledge that you have done so:

ACTION NEEDED: Acceptable Use Agreement

- Alternatively, you may scan this QR code to go to the form
- Please keep a copy of the Acceptable Use Agreement for your reference.

Appendix E

Pre-Prep Pupil E-Safety Agreement

Our key principles for online safety are:

1. **Be careful**
2. **Be kind**
3. **Tell someone**

Keeping me Safe at home and at school

We check with a grown up before using apps or the internet.

We tell a grown up if something makes us feel worried.

If we get stuck or lost when using technology we will ask for help.

We can write polite and friendly messages to people we know

We will keep our personal information, our name, address, our school, our pictures "Top Secret" and not share on the internet.

We will not bring mobile phones or other electronic devices (e.g. tablets, ipods and games consoles) to school.

Pupil Agreement

I have listened to and understood the pupils' e-safety agreement and I will follow the rules which are there to keep me and the school safe.

Appendix F

SOCIAL MEDIA POLICY

1. OVERVIEW AND PURPOSE

1.1 Introduction and scope

Caterham School encourages staff and those holding official volunteer roles to use social media within the boundaries of ensuring that all school related posting is appropriate, safe, within the law, maximises impact and highlights individuals and the school and the school community in an appropriate way.

Social media channels offer great opportunities to communicate and engage with a wide range of stakeholders, including current and prospective families, alumni, external collaborators and the wider global Caterham School community. They also provide professional opportunities for alumni and parents, a way for teaching staff to connect on professional topics, and usage of social media has become a common part of everyday life.

However, some inexperienced social media users sometimes think, incorrectly, that online activities, whether on open or closed networks, operate outside normal expectations and laws of engagement. There are risks associated with the use of social media which can impact on the safety, health, and wellbeing of individuals and also on the reputation of the school. Additionally, misuse of social media can amount to unlawful activity and/or contravene school policies. The law of defamation applies to social media activity just as it does to other media. The School's reputation is a vital part of Caterham's ongoing success and social media plays an important role in maintaining it. Members of staff and members of the school community holding official volunteer roles, including but not limited to Trustees, Foundation Members, Old Caterhamians Association, PA Committee members andPA Reps, need to separate school content so that personal content is not pushed out on any channels that are, or might naturally perceived to be representing the school or the wider school community. Members of the school, both staff and official volunteers should also be cautious about the ability to separate their work and personal personas which is not easily possible on social media (what you say on your personal channels could affect your work life and/or your role as an official volunteer or representative of the school community).

1.2 The key objectives of this policy are to:

- Provide staff and those holding official volunteer roles with information on the School's requirements and expectations regarding social media use, including responsibilities of users of School social media accounts include those accounts aligned to the wider School community
- Outline some of the potential legal risks associated with improper use of social media

- Ensure a consistent approach to social media usage across the entire School community
- Set out the responsibilities of users of School social media accounts
- Ensure staff and official volunteers protect their personal security and the security of School information assets
- Outline channels for escalation of issues or concerns
- Signpost staff and official volunteers to resources which will support them in enhancing the social media presence of the School.

2. SCOPE

2.1 All Caterham School (including Prep School) staff and volunteers holding an official role within the school are covered by and must adhere to this policy.

2.1.1 Pupils

Private accounts or profiles that don't refer to the School (either implicitly or explicitly) fall outside these guidelines, as do our pupils' personal use of social media. When using social media, in either a personal or professional capacity, we also ask our community to remember the School's values and high standards of behaviour.

2.1.2 Staff

School staff are influential among many audience groups including the local area, local and education media as well as within our own school community. As such, conduct yourself on social media in the same way you would if you were meeting these groups in person and representing the School.

2.1.3 Official Volunteers

The School benefits from the support of official volunteers, including the School's Trustees, Foundation Members and committees including the Old Caterhamians Association and the Parents Association and PA Reps. To maintain the reputation of the School all official volunteers using School social media channels or channels which represent constituent groups of the school community must uphold the School's reputation and abide by the School's key messages. Social media channels representing constituent groups of the school and/or channels operating under school brands or sub brands must assign ownership of the account to the Director of External Relations or a member of the External Relations team.

2.2 Social media

Social media refers to websites and applications that enable users to create and share content or to participate in social networking whether open or closed platforms. This policy applies to all social media sites and networks. Examples of popular social media sites include, but are not limited to:

LinkedIn, Twitter/X, Facebook, YouTube, Instagram, TikTok, Snapchat, Weibo, WeChat, WhatsApp.

3. RESPONSIBILITIES

3.1 All Users

Staff and school community representatives' presence on social media is a public record. Digital footprints, in the form of comments or activity, can be recalled at any time, impacting on an individual and the School's reputation. Social media should be a positive tool, but it is important to carefully consider post content and account security to mitigate against negative risks.

Posting inappropriate, offensive or unlawful material on social media can have serious consequences, including:

- long-term impacts on an individual's employment prospects
- legal action
- the School taking disciplinary action
- significant damage to the School's reputation

Inadequate account security can lead to hacking and identity theft which also have serious legal, reputational, academic, employment and financial implications.

3.2 Staff

As a member of staff using social media relating to the School, you should read this policy in full and ask for clarification where necessary.

3.2.1 Staff are authorised to make appropriate and reasonable use of social media from Caterham School equipment in line with the School's IT and other related policies.

3.2.2 Personal and professional accounts

Social media can be an important tool for colleagues' professional activity and provide a great platform for raising awareness and enhancing personal networks. It is recommended that colleagues using social media for both professional and personal reasons maintain separate accounts for these purposes as the audiences for each activity are usually distinct. Personal and professional accounts held personally should not use Caterham School branding or sub branding. Where your professional role or official connection to Caterham School could be identified, you should include an appropriate disclaimer, such as: "The views expressed here are my own and do not necessarily reflect the views of Caterham School."

Caterham School does not and will not monitor individuals' personal accounts. However, if concerns are raised regarding content posted on a staff member's osocial media account and the post is considered to amount to misrepresentation of the School's position or

represents misconduct, the School has the right to request the removal of content.

3.3 Volunteers holding an Official Role within the School Community

As a representative of the School community using social media which relates to the School, you should read this policy in full and ask for clarification where necessary

3.3.1 Official volunteers are encouraged to engage with social media to support the work of the School, its aims and wider community in line with the current values of the School

3.3.2 Official volunteers are encouraged to use official school channels where provided in preference to closed networks, for example PA Reps should use the Classlist platform provided for the Parents' Association activities over WhatsApp.

3.3.3 Personal and professional accounts

Social media can be an important tool for the wider school community, and for volunteers' professional activity and provide a great platform for raising awareness and enhancing personal networks.
Personal and professional accounts held personally should not use Caterham School branding or sub branding and must be distinct from official school accounts. Where your official role with Caterham School could be identified, you should include an appropriate disclaimer, such as: "The views expressed here are my own and do not necessarily reflect the views of Caterham School."

Caterham School does not and will not monitor individuals' personal accounts. However, if concerns are raised regarding content posted on an official volunteer's social media account and the post is considered to speak against the position of Caterham School, amount to causing damage to the School's reputation or speaks directly against the purpose and high standards of the School, the School has the right to request the removal of content. Where access to and/or engagement with school social media platforms has been granted the School retains the right to remove it.

4. POLICY

4.1.1 Use of social media by the community

Caterham School's policy framework commits to ensuring a safe and welcoming environment in which all pupils and staff thrive and achieve their full potential. It expects all staff, volunteers and pupils to act in line with these commitments. When posting on social media, staff and official volunteers must demonstrate respect for pupils, school staff and property, and for members of the wider community and act in accordance with the School's values.

When posting on social media, staff and official volunteers must not:

- post or promote content which damages, or has the potential to damage, the School's relationships with and standing in the local community or other outside bodies or organisations
- fraudulently assume the identity of another person
- post or promote content which harasses, bullies or intimidates; is intended to incite violence or hatred; is abusive in relation to another person's protected characteristics, religion or belief, race, disability or age
- breach others' privacy through sharing or promoting private information, images or other content
- repeatedly make unwanted or unsolicited contact with another person
- misuse the School's branding or imagery on personal social media sites whether open or closed.

The School regularly moderates comments across our channels. We are committed to freedom of speech and expression which are principles protected in law but reserve the right to delete comments on posts on which consist of hate speech, bullying, offensive language (either through sentiment or the use of expletives). In a small number of cases, when it's in the interest of our wider audience, the School may take the decision to block users.

4.1.2 It is never acceptable to use social media to attack someone's character or conduct or make derogatory comments about them including because of their views, opinions or beliefs exercised in accordance with the law. To do so could stray into behaviour that amounts to bullying, harassment or intimidation It may also be a breach of the civil or criminal law.

4.1.3 Any disclosure of wrongdoing, serious malpractice or impropriety should be raised by contacting the Headmaster or Bursar. In the instance of a former employee releasing such information through a social media channel, the School's Whistleblowing policy will be initiated before additional action is taken.

4.3 Legal risk

There are a raft of legal issues relating to social media ranging from defamation, where untrue content affecting a person's or organisation's reputation is posted, which causes, or is likely to cause, harm. Harassment, where someone is subjected to conduct, causing distress or alarm, including stalking, trolling and cyber-bullying. Intellectual property infringement, where content copies a substantial part of a work protected by copyright resulting in financial loss for the subject or malicious falsehood where lies and damaging content are posted with an improper motive. A list of relevant U.K. legislation is listed at the end of the policy

4.4 The Media

If you are contacted by a journalist or other media source to comment on activities related to the School please speak to the Director of External Relations as quickly as possible. They can support you and give you expert guidance about how to respond.

4.5 School Social Media Accounts

4.5.1. Establishing new School social media accounts

There are near 30 social media accounts including school, departmental and community accounts, across all platforms, with most regularly posting online. Updated guidance and best practise is shared with staff running these accounts each term and support is always available at any time from the External Relations department. If you are setting up a school or school community channel and are a member of staff or an official volunteer you must contact the External Relations team before starting. They can help you make best use of your presence and ensure you adhere to brand guidelines and messaging. Before establishing a new account, staff should consider whether their audiences and objectives cannot be met through an existing account. Official School accounts must not be established or run by pupils. The School retains the right to refuse the setting up of new chool or school community channel.

The name of any new account should always begin with @Caterham or at the very least mention Caterham in their handle. The official hashtag uniting all Caterham content is: #MyCaterham

4.5.2 Management of accounts

All School social media accounts must adhere to the School's brand guidelines and give clear indication of their purpose. If several members of staff run the same social media account, a designated account manager should be agreed and have a system in place to regularly monitor, update and manage the content of any official School account and ensure questions posted are responded to promptly. If negative comments are posted by viewers please contact the External Relations department for support.

4.5.3 Posting from School accounts

All social media posts from Caterham School accounts represent the institution. It is important that every post is carefully considered, appropriate and designed to enhance the reputation of the School. If possible, measures should be put in place to avoid communication errors, including checking of content by a third party.

Anyone posting on school accounts will be viewed externally as representing the institution. All content posted or otherwise promoted must be courteous and respectful of others inside the school and in the wider community. Staff should remember the power imbalance they hold with pupils and should be wary of negative interactions which may be interpreted in a way different to that intended.

Care should always be taken to ensure the content is properly considered and not in breach of the civil or criminal law before it is posted. Social media content must not:

- discuss the inner workings of the School or reveal future plans or ideas that have not yet been made public.
- contain private or confidential information regarding an individual, company or organisation or about the School itself.
- reveal details of intellectual property belonging to the School.
- breach any confidentiality rules pertaining to the School.
- identify a pupil other than using their first name and use or share pupils' images without checking permission is given (as available on iSams)

The School reserves the right to remove content on School and school community channels.

4.6 Account Security

Account hacking represents a significant risk to social media accounts and can lead to the spread of harmful misinformation and extensive reputational damage for the host organisation and individual community members.

Every School and school community account must have an agreed manager with responsibility for choosing strong, secure passwords. Passwords should be securely stored, not in files on shared drives or on paper. The current passwords for all School and School community accounts must be sent to the Director of External Relations.

In cases of emergency, such as hacking, the school's External Relations team may need urgent out of hours access to any School or school community social media account.

It is good practice to regularly renew passwords. Staff should also secure accounts with 2-factor authentication.

If more than one member of staff has access to the account, the account manager is responsible for collating and maintaining a log of staff with access to the account's password and the password must be changed whenever one of those staff members moves on to a different role or different institution.

4.7 Concerns, issues & crisis situations

4.7.1 Concerns & issues

If a School account has been hacked, or a post is attracting negative comments and it is not clear how to respond, staff should flag with the External Relations team and seek advice. Social media activity on staff or pupils' accounts that raises welfare concerns should be reported in line with the School's Safeguarding policy. Social media activity on pupils' or staff accounts which constitutes misconduct should also be reported in line with the School's Staff Code of Conduct Policy.

4.7.2 Crisis Situation

Social media provides a vital channel for critical information for staff, parents, pupils and wider stakeholders during a crisis situation and/or an emergency. It is vital that the information provided is timely, consistent and accurate.

All communications on social media from the School in a crisis will be issued via the School's central social media accounts operated by the External Relations department.
In order to minimise the risk of issuing conflicting and/or incorrect information, it is vital that all other school and school community social media accounts do not post information or updates during or following a live incident. They must point to the school centre social media accounts and may repost official content put out on these channels.

4.8 Permissions

The act of liking, posting or sharing content can be viewed as an endorsement, so ensure what you are posting, or sharing is in line with our School's values.

Before you share content from a social media account:

- try to validate the authenticity of the account you want to share content from – for example, look for the blue tick on Twitter, read the biography on their page or scroll through posts and photos to see if they are the kind you expect to see
- ensure the social media account is the original rights-holder of the content you want to share – and if they aren't, ask who is and contact them directly to seek permission
- ask the social media account permission to share their content on the platforms you're planning to use and include a credit line, unless you're sharing directly on the platform you found the content, such as a retweet.
  It's especially important not to publish content or contact details of staff or pupils without their express permission. Pupils' consent to be photographically featured can be found on iSams. Before taking a school trip or activity it is strongly recommended that all pupil participants' photo consent is checked prior to the trip taking place.

If you need more advice or guidance, you can contact the External Relations department.

Appendix G

Pupil Social Media Policy

Introduction

The internet provides a range of social media tools that allow users to interact with one another, currently, platforms such as Instagram and Snapchat are popular with teens and young adults, however the School is conscious that trends can change rapidly and goes to great lengths to monitor and adapt to changes.

While recognising the benefits of these media as new opportunities for communication, this policy sets out the principles that Caterham School pupils are expected to follow when using social media.

The principles set out in this policy statement are designed to ensure that pupils use social media responsibly so that they protect themselves whilst also maintaining the school's reputation.

This policy statement also aims to help pupils understand that it is necessary to distinguish the use of social media for personal reasons to the use of social media in connection with the school or for professional reasons.

Scope

This policy applies to pupils of Caterham School.

This policy covers personal use of social media as well as the use of social media for official Caterham School purposes.

This policy applies to personal web presences such as social networking sites (for example *Instagram*) blogs, microblogs, and messaging platforms (such as *Twitter and Snapchat)*, chatrooms, forums, podcasts, open access online encyclopedias (such as *Wikipedia*), content sharing sites (such as *YouTube*), and anonymous posting sites (such as *Saraha*). The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the platform.

Use of Social Media in School

The school maintain presences on various social media sites as they provide very effective additional channels of communication with parents/ carers, pupils and the wider community.

For example, Twitter and Instagram are used to collate and publicise a stream of positive messages about the multitude of activities that go on at Caterham School every day. As a pupil you may be encouraged to follow one of these accounts (a subject's Instagram feed for example). You should be aware of the expected behaviours associated with this action.

Social Media Policy Statement:

- Pupils may not upload video or photo content to any hosting services (such as YouTube) without explicit permission from their teacher, and even then, they may not tag the school or list the content 'publicly'. All uploaded media should remain 'unlisted' and free from tags. If you are unsure of how to do this, then you should seek help. It is highly unlikely that it would be acceptable for you to upload content to a non-school site or page, so please do not expect to do this. Please be aware that being off site does not relinquish these restrictions in any way.

- Pupils may not comment on videos or other social media postings about the school unless they are doing so in a positive fashion. The language used should be carefully chosen. If you are unsure if a post is appropriate, then this should indicate that it would be better not to post it at all.

- Under no circumstances may you upload images or video of teachers or other pupils without explicit permission. Indeed no such images should be held on your iPad or personal devices at any time without a clear reason for having them.

- You should not identify members of the school community in any posts to social media. If posting for school purposes, you may name yourself or other pupils by first name only and you should never reveal your location if it is outside of the school site.

- Strong password security must be maintained and regularly changed for any social media account, to prevent it from being hi-jacked and misused. Passwords should never be written down. A combination of upper and lower case characters should be combined with numerals.

Personal Use of Social Media

It is entirely acceptable for members of the school community to have personal social media accounts, as long as they meet the age requirements of the site they are signing up to. The staff at Caterham School do not actively search pupils' personal accounts, (unless there is a serious reason to do so for a member the Safeguarding Team to do so), and we wish you to enjoy all of the many benefits of having such online presences. However, it is also important for you to understand that as your use of these tools becomes more pervasive, it is to be expected that we will become more aware of them and that often what happens at school is explored further online. If comments or behaviour online is seen to put the school in a negative light, or pupils are showing a lack of care and consideration to others, you should expect the school to intervene.

It is worth considering that information (text, images, video) held on social media platforms;

- is never completely private and can very easily enter the public domain
- can be misinterpreted by audiences it was not originally intended for
- may persist beyond your wishes
- might be copied and used by third parties without your consent

Personal Use of Social Media Policy Statement

- Pupils are advised not to identify themselves as members of Caterham School in their online profiles. This is for safeguarding reasons, but also to help avoid connecting your personal comments back to the school unnecessarily.

- You should not, under any circumstances 'follow' a teacher or other member of staff on social media, unless this is done through an account which has been created for school purposes and is for your benefit. Attempts to do so will be rejected, but persistent attempts to do so may be dealt with more seriously. If a member of staff requests to 'follow' you on social media you should report this immediately to your Head of Year or Mrs Fahey .

- Pupils should be aware that making extreme political, religious or philosophical comments on social media may attract unnecessary attention and require the school to intervene.

- Pupils should not use social media to document or distribute evidence of activities in their private lives that may bring the school into disrepute.

- Pupils must not use social media to bully other members of the school community. This may be through the sharing of images, the use of unkind or discriminatory language or at times, through deliberate exclusion.

- Pupils must not use social media to bully or elicit negative reactions from those outside of the school community, in particular, but not exclusively, if the school's identity is associated with the posting.

- You may not, under any circumstances create social media accounts that purport to be official Caterham School accounts, or represent the views of the school or members of its community in any way.

- School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

- Pupils must not edit open access online encyclopaedias such as Wikipedia in a personal capacity from school.

- Pupils must not use social media and the internet in any way to attack, insult, abuse or defame anyone who is a part of the school community; such action will be taken very seriously. Where there is suspicion that libel laws may have been broken the police may be called.

- Pupils are strongly advised to ensure that they set the privacy levels of their personal sites to be as strict as possible and to opt out of public listings on social networking sites to protect their own privacy.

Appendix H

Online Safety Expectations

These expectations help pupils to protect themselves and the school, by outlining what is and isn't acceptable when using school technology.

Pupils are reminded that the school owns the computers, iPads, and network, and sets the rules for their use. Misuse can be a criminal offence.

- I will only use school IT systems (internet, email, iPads, etc.) for school-related purposes unless given permission by the Headmaster.
- I will not use school IT for personal gain, gambling, political activity, advertising, or illegal purposes.
- I will log in only with my own username and password and keep my password private.
- I am responsible for all activity under my username.
- I will use only my school email address for school-related work and communicate respectfully.
- I will not send anonymous or chain messages.
- I will act responsibly online, using appropriate language and carefully selecting the resources I access.
- I appreciate that other users might have different views to my own and will contribute positively to public discussion.
- I will not share personal details (name, phone, address) online.
- I will not meet online contacts in person without school or parent approval.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal and will report anything inappropriate.
- I understand that creating, taking, sharing or saving nude or semi-nude images/ videos of anyone under 18 is illegal.
- I will not download or install software or try to bypass the School's Wi-Fi or filtering and monitoring system.
- I will ensure that my online activity, in and out of school, do not cause distress to others or bring the school into disrepute.
- I will respect the privacy and ownership of others' work online at all times.
- I will only use AI to enhance and develop my work when specifically permitted by my teacher, using school approved AI tools and will be transparent about this when work is submitted.
- I understand that phones and smart devices should not be visible or disrupt learning during the school day.

Pupils should understand that the school may monitor and log online activity for safety and legal reasons.

Pupils should understand that breaking these expectations can lead to sanctions, the loss of my internet access or iPad and that parents/carers may be contacted.

Appendix I

IT Acceptable Use Policy for the use of school laptops

As a member of the Caterham School community, your use of technology should be respectful, responsible, and safe - reflecting positively on yourself and the school.

Your online presence (digital footprint) should be a positive one, as should your use of technology in school.

The following statements form the *Pupil Acceptable Use Policy: School Laptops off site*

- I understand that the main Acceptable Use Policy for 6th Form pupils applies at all times, to this device and any other used in school, or provided by the school.
- I understand that the only permissible use of the laptop is to complete work for my studies, specifically the use of the Adobe suite for Photography and Art work.
- I understand that I am responsible for saving work to OneDrive and deleting any local copies of my work, and that if I fail to do so, another user may delete my work which may not be recoverable.
- I understand that the school owns the laptop and that I have a responsibility to take reasonable precautions to look after it. Damage to the device that requires repair will result in a £100 charge which will be added to the school bill for the following term.
- Damage to the device caused by water from a sink, bath or similar will result in a charge for the full cost of replacement, as this will not be covered by our insurance policy. This cost will be £560 and added to the school bill for the following term.
- I will not attempt to install any additional software, not delete anything that is already installed on the laptop.
- I have read and understood the school's sanctions policy for device misuse.

I will follow these guidelines both in and out of school for as long as the device is being brought into the school environment.

Pupil Name: …….

Pupil Signature: …….

Parent/Guardian Name: …….

Parent/Guardian Signature: …….

Date: ……

Appendix J

Caterham School AI Policy

Caterham School embraces the opportunities offered by Artificial Intelligence (AI) while ensuring its use remains ethical, safe, and educationally purposeful. This summary outlines our core expectations for both staff and pupils.

Approved AI Tools

- RileyBot is the default AI tool for pupils. It is designed to promote safety, provide personalised support, and foster independent learning, including revision help, project planning, and feedback.
- ChatGPT (OpenAI) is permitted for staff use only. It may be used to support planning, marking, communication, and professional development. Pupils are not permitted to use ChatGPT under any circumstances.

Expectations for Pupils

- AI must not be used to cheat, impersonate others, or to input personal data.
- Only school-approved AI tools, such as RileyBot, may be used. Public tools like ChatGPT are strictly prohibited for pupil use.
- Pupils are expected to be transparent about any use of AI in submitted work or learning tasks.

Expectations for Staff

- Identifiable or sensitive information must never be entered into public AI platforms.
- AI-generated marking or feedback must always be reviewed by staff before being shared with pupils.
- Staff are responsible for ensuring any AI-enabled tool or platform used with pupils is age-appropriate, compliant, and used transparently.
- Staff must also be open about their use of AI, particularly when it supports teaching, assessment, or communication.

Ethical Use

- All AI use should promote fairness, inclusion, accountability, privacy, and critical digital literacy.
- Pupils are supported in their understanding of misinformation, bias, and ethical AI use through the EDGE curriculum, tutor time, and subject lessons.

This summary should be read in conjunction with the School's IT Acceptable Use Policy.