Online Safety Policy

CATERHAM SCHOOL

CATERHAM PREP

Policy Authors:	Adam Webster (Deputy Head Innovation) Louise Fahey (DSL)
Date Reviewed By Authors:	September 2023, with Principal Deputy Head, Deputy Head (Prep) and Head of the Pre-Prep
Next Review Due:	September 2024

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 an industry leader in this field. Caterham School remains recognised as an Apple Distinguished School and, in 2018, was awarded the TES Independent Schools Award for 'best use of technology.' All staff and pupils are given an iPad (from Prep Year 3 up, with shared use below) to support and enhance their learning, supported by a powerful infrastructure including excellent Wifi, cloud storage and interactive boards and Apple TV in every classroom. The school is eager for pupils to make the most of the opportunities afforded by the use of technology but does so with the safeguarding of every child's welfare at the heart of every decision.

This policy should be read in conjunction with the following documents:

- Safeguarding Policy
- Keeping Children Safe in Education 2023
- NMS 2023
- Wellbeing Policy
- Behaviour Policy
- Anti-bullying Policy
- 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)
- KS1 Pupils E-Safety Agreement (Appendix F)
- Staff Social Media Policy (Appendix G)
- Pupil Social Media Policy (Appendix H)
- Online Safety Rules (Appendix I)
- Mobile Phone Policy (Appendix J)
- Remote Working Guidelines (Appendix K)
- Important Information about your use of ICT (Appendix L)
- Laptop Acceptable Use Policy (Appendix M)
- AI Policy (Appendix N)

The 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.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk, content, contact, conduct and commerce.

Pupils increasingly use electronic equipment on a daily basis to access the internet, share and view content and images via social media sites and interact online. Many children now have unlimited and unrestricted access to the internet via mobile networks - 3G, 4G and now 5G - which some of them may abuse to sexually harass their peers, share indecent images consensually and non-consensually and view and share pornography and other harmful content. Online access can also be misused to send hurtful or abusive texts or emails, and to groom and entice children to engage in extremist, criminal or sexual behaviour such as webcam interaction or face-to-face meetings.

Pupils may also be distressed or harmed by accessing inappropriate material such as pornographic websites or those which promote extremist behaviour, criminal activity, suicide or eating disorders.

Boarding: 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 the mobile networks listed above 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 Y10 inclusive hand their devices in at bedtime, while our Y11, 12 and 13 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).

All pupils are taught about online safety throughout the curriculum and all staff receive online safety training which is regularly updated. The DSL has lead responsibility for online safety. The member of the Senior Leadership Team with responsibility for ensuring standards are met is Adam Webster (Deputy Head Innovation). The Trustee with responsibility for online safety is Deborah Grimason.

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

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 Online Safety policy forms part of the safeguarding policies, as well as being the overarching document supporting the suite of IT policies. It is compiled by the DSLs and reviewed regularly in line with regulatory change and developing technological trends.

Teaching and learning

The internet is 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 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 through our VLE, 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.

The school internet access is provided by Virgin. Our filtering system is appropriate to the age of pupils: the providers are acknowledged industry leaders in their field. Pupils are taught what internet

use is acceptable and what is not and are given clear objectives for internet use; they are educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. They are shown how to publish and present information appropriately to a wider audience and are taught how to evaluate internet content and how to validate information before accepting its accuracy. Above all the School endeavours to ensure that pupils are critically aware of the materials they read. The school always seeks to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Pupils are taught how to report unpleasant internet content, for instance by using the CEOP Report Abuse icon. In rare cases where pupils' parents lack economic or cultural educational resources, the school builds digital skills and resilience, acknowledging the lack of experience and internet at home. For children with social, familial or psychological vulnerabilities, further consideration is taken to reduce potential harm.

Virtual Learning Protocols & Safeguarding

In response to new ways of working which have emerged since Covid, all parents are asked to give consent for teachers and pupils to meet virtually 1-to-1 in order to work or participate in 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 son/daughter)

Managing Internet Access

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

E-mail

Pupils and staff may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive an offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Staff to pupil email communication must only take place via a school email address or from within the learning platforms (Firefly & Microsoft Teams) 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.

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.

Publishing pupils' images and work

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, such as the School's Twitter feed, particularly in association with photographs. Permission is sought in line with our general Privacy Notice which can be found on the school website, updated recently to be GDPR compliant.

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 are explored in the pupil ***Acceptable Use Policy*** and the pupil ***Social Media Policy*** found in the appendix of this document. Much time is spent educating pupils 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 2023 and its relevant additional documentation.

Parents and pupils are offered guidance on the safe use of social media through a bespoke initiative called the Caterham Online Partnership, a series of pages found on Firefly. These pages contain practical steps that can be taken to provide age-appropriate filtering, as well as guidance on what to do if inappropriate content is disseminated online. There is also guidance for parents on how to begin an open, productive discussion about online safety with their children.

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, IT Department 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.

A daily report is compiled by the School's filtering provider Sophos and sent to the DSL, Deputy Head (Innovation), Deputy Head/ DSL (Prep School), Assistant Head (Boarding) Head of Wellbeing which lists all searches made by the school community which reach a safeguarding threshold. The categories listed are: Suicide, Self-harm, Pornography, Drugs, Weapons, Violence and Intolerance. 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.

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
- 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

Youth produced Sexual Imagery

Youth produced sexual imagery, problematic or harmful sexual behaviour and child on child abuse can all happen online. If staff are concerned that an incident of this nature has taken place, 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 2023 and in the UK Council for Internet Safety's 'Sharing nudes and semi-nudes' which can be found here. Under no circumstances should images be viewed.

Creating or sharing explicit images of anyone under 18 is illegal. The School will respond swiftly to ensure pupils are safeguarded, supported and educated.

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 pupils' age.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones and associated cameras, such as those in pupils'

iPads, will not be used during lessons or formal school time except as part of an educational activity – for instance, making a film of a scene from a Shakespeare play in English lessons. The sending of abusive or inappropriate text messages is forbidden. Mobile and smart technologies, including wearable technology, games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school. Further detail on this matter is explored in our ***Mobile Phone Policy*** found in the appendix of this document.

Staff and pupils are expected to engage with the school's Virtual Learning Environments, Firefly and Microsoft Teams, in a positive and productive way, in line with the ***Staff and Pupil Acceptable Use Policies***.

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

Protecting personal data

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

POLICY DECISIONS

Authorising internet access

All staff must read the ***Acceptable Use Policy for Staff and Trustees*** before using any school IT resource. The school will maintain a current record of all staff and pupils who are granted access to school IT systems. In Early Years and Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials: parents will be asked to sign and return a consent form. All Prep pupils and parents are provided with a copy of the relevant Acceptable Use Agreement (see Appendices) at the start of each academic year. Senior School pupils must apply for internet access individually by agreeing to comply with the pupils' ***Acceptable Use Policy***, which includes internet protocols. 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.

Any person not directly employed by the school will be directed to the Acceptable Use Policy for Visitors.

Assessing risk

The School takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School cannot accept liability for the material accessed, or any consequences of internet access. The School monitors carefully IT trends, changes and updates to establish if the Online Safety Policy is adequate and to ensure that the implementation of the Online Safety Policy is appropriate and effective.

COMMUNICATION

Introducing the Online Safety Policy to pupils

Appropriate elements of the Online Safety Policy are shared with pupils via the pupil ***Acceptable use Policy*.** Tutor sessions and Wellbeing at the start of the school year revisit the Acceptable Use Policy and ensure pupils understand expectations. ***Online safety rules*** will be posted in all networked classrooms and sent to all pupils. Pupils are routinely informed that network and internet use will be monitored, and a range of curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils through the Wellbeing curriculum, as well as updates on an ad hoc basis through assemblies and the Caterham Online Partnership.

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 acknowledge 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.

Enlisting parents' support

Parents' and carers' attention will be drawn to the School's Online Safety Policy in such formats as the newsletter, the School web site and the Caterham Online Partnership. The school will ask all new parents to sign the parent /pupil agreement when they register their child with the School.

Parents should be given access to online safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust. The School performs this duty with face-to-face meetings and via the Caterham Online Partnership.

Often children do not wish to be constantly online but lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible, to interact with their children on the internet as well as provide other opportunities for learning and recreation.

Appendix A

IT Acceptable Use Policy for Staff and Trustees

IT and related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff, including those in the EYFS setting, are aware of their professional responsibilities when using any form of IT. All staff are expected to adhere to this policy at all times. Any concerns or clarification should be discussed with the DSL, Deputy Head (Innovation) or Principal Deputy Head.

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

- I appreciate that IT includes a wide range of systems, including my iPad, mobile phones, PDAs, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that it may be a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the school's email, internet, learning platforms such as Firefly and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headmaster or Board of Trustees.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data (such as data held on iSAMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Hard copies of sensitive personal data should only be taken out of school when authorised by the Headmaster or Board of Trustees. Sensitive personal data should not be transferred to external hard drives, including USB sticks.
- When working away from the school site, I will refer to the guidelines given in the Remote Working policy, which can be found in Appendix K of this document .
- I understand the importance of protecting and monitoring my use of data in line with GDPR regulations. In particular, I will adhere to the school's policy on the creation and retention of personal data and will refer to the school's Privacy Notice, the GDPR working party or the Principal Deputy Head should I be unsure of what data I can hold.
- I will not install any hardware or software without the permission of the Deputy Head (Innovation) or IT Systems Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that my use of the internet and email, when accessed through the School network, can be monitored and logged and can be made available, on request, to the Headmaster, and that School-owned devices, such as iPads, can be scrutinised at the Headmaster's request.
- 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 audio recordings of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and (where appropriate) with written consent of the parent, carer or staff member. Images and audio recordings will not be distributed

outside the school network/learning platform without the permission of the parent/carer, member of staff or Headmaster.

- I will ensure that my online activity will not bring the School into disrepute.
- I have read the ***Staff Social Media Policy*** and I understand and agree to its content.
- I will strive to ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and 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 promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that I have understood the protocols around video conferencing pupils, and in particular, in conducting 1-to-1 meetings with pupils, in line with our Safeguarding Policy
- I will report any incidents of concern regarding children's safety to the DSLs or the Headmaster.
- I understand that sanctions for disregarding any of the above will be in line with the School's disciplinary procedures and serious infringements may be referred to the police.
- I understand that this policy will be updated regularly, in line with policy changes within or outside of school and that it is my responsibility to read new versions of this document.

Accompanying documents to read:

- Online Safety Policy
- Remote Working Policy
- Staff Social Media Policy
- Pupil Acceptable Use Policy

Appendix B

IT Acceptable Use Policy for Pupils (1st-5th Year)

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. 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.

The following statements form the Pupil Acceptable Use Policy:

- I understand that the school owns the computer network and the iPad I have been given and can set rules for its use. I understand it is a criminal offence to use a computer or network for a purpose not permitted by the school.
- 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 choose usernames that are appropriate and consider carefully what personal information I give out about my life, experiences and relationships.
- I will not be obscene either in the words that I use or the content that I view. This includes material that is violent, racist, sexist or adult in nature.
- I will also respect the laws of copyright and ensure that sources used are referenced.
- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or my location and will tell an adult should someone ask me for these details.
- I will not take or distribute any images or video of people without the consent of my teacher or without their explicit consent.
- I understand that it is against the law to take, save or send nude or semi-nude images or videos of anyone under the age of 18.
- I will never use my device to bully or upset anyone and will report any instances of bullying that I come across.
- I will use my device as directed by my teachers and will do nothing to bring the school into disrepute.
- I will only use my school email address for school-related work, and where appropriate, I will use the alias email address I have been given.
- I will not send anonymous messages or chain mail.
- I will not attempt to circumvent the school's filtering 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 only be connected to the 'Caterham Wifi' network.

- First to Fifth year pupils should not have any other devices connected to the network unless permission has been granted from the SENDCO or their Head of Year.
- I understand that viewing/reading/modifying/storing/editing any HTTP or HTTPS internet traffic, or any other attempts to retrieve personal data that has been stored digitally is totally unacceptable.
- I will only ever use my own account (Please note that sharing your logon details with others will be dealt with as an equally serious offence as using another person's account).
- I will not attempt to modify static IT equipment.
- I understand that torrenting, peer to peer networks or illegal file sharing are not permitted
- Social media may only be used at the discretion of my teacher in consultation with the Senior Management Team.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher.
- Profiles created for school-based accounts will use the anonymized (numerical) emails given to me. I will not use real photographs of myself or other pupils as an avatar, and where possible I will give reduced personal information such as my first name and first initial of my surname. I should speak to a member of staff about creating these accounts if I am unsure.
- I understand the behaviour expected when meeting with teachers and pupils virtually for the purposes of learning
- When using Microsoft Teams, I will only use the Chat facility when required for my schoolwork.
- I will not record (which includes audio and/or video) any part of a lesson, physical or virtual, with any device unless this has been agreed with my teacher.
- I will not contact my teacher or anybody else using video or voice chat, unless for, or about, a specific task requested by my teacher.
- I will only join Team Meetings during the allocated times and will not access them before a meeting starts or after it ends.
- I will not have one to one conversation with anybody else via audio or video, except in circumstances discussed and agreed between my parents and teacher, and only then with an adult in the room with me.
- The playing of games is not permitted whilst on the school site.
- I will remain signed into my school-given iCloud account (ending @appleid.caterhamschool.co.uk) at all times.
- I will acknowledge and adhere to the ***'online safety rules'*** posted in classrooms around the school.
- I have read the document ***'Important Information about your use of ICT'*** and agree to follow its guidance.
- I have read and understood the school's sanctions policy for device misuse.

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

This document and related IT policies and guides are available on the school's website and Firefly and will be regularly updated in line with DfE guidance. At the start of each academic year all pupils undertake the online quiz which involves reviewing this document with their tutor or in curricular wellbeing, and finished with a sign-off agreeing to the terms of present and future amends of this document and related policies that ensure the safeguarding of the pupils.

Appendix C

IT Acceptable Use Policy for 6th Form

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. 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.

The following statements form the *Pupil Responsible Use Policy: 6th Form BYOD Version*

- I understand that whilst I am providing my own device for use at school, my use of this device is still subject to a range of conditions as set out below and breaching these conditions may result in sanctions including the removal of WiFi 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 that the device I am using for school purposes is signed into OneDrive and has my school email account setup on it at all times.
- I will ensure I have a device/process in place to access Firefly at all times.
- I understand that the school owns the computer network, including the WiFi network and sets rules for its use. I understand it is a criminal offence to use a computer or network for a purpose not permitted by the school.
- 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 choose usernames that are appropriate and consider carefully what personal information I give out about my life, experiences and relationships.
- I will not be obscene either in the words that I use or the content that I view. This includes material that is violent, racist, sexist or adult in nature.
- I will also respect the laws of copyright and ensure that sources used are referenced.
- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or my location and will tell an adult should someone ask me for these details.
- I will not take or distribute any images or video of people without the consent of my teacher or without their explicit consent.
- I understand that it is against the law to take, save or send nude or semi-nude images or videos of anyone under the age of 18.
- I will never use my device to bully or upset anyone and will report any instances of bullying that I come across.
- I will use my device as directed by my teachers and will do nothing to bring the school into disrepute.
- I will only use my school email address for school-related work, and where appropriate, I will use the alias email address I have been given.
- I will not send anonymous messages or chain mail.

- I will not attempt to circumvent the school's filtering 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.
- You may only be connected to the 'Caterham Wifi' network.
- I understand that viewing/reading/modifying/storing/editing any HTTP or HTTPS internet traffic, or any other attempts to retrieve personal data that has been stored digitally is totally unacceptable.
- I will only ever use my own account (Please note that sharing your logon details with others will be dealt with as an equally serious offence as using another person's account).
- I will not attempt to modify static IT equipment.
- I understand that torrenting, peer to peer networks or illegal file sharing are not permitted
- Social media may only be used at the discretion of my teacher in consultation with the Senior Management Team.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher.
- Profiles created for school-based accounts will use the anonymized (numerical) emails given to me. I will not use real photographs of myself or another pupil as an avatar, and where possible I will give reduced personal information such as my first name and first initial of my surname. I should speak to a member of staff about creating these accounts if I am unsure.
- I understand the behaviour expected when meeting with teachers and pupils virtually for the purposes of learning
- When using Microsoft Teams, I will only use the Chat facility when required for my schoolwork
- I will not record (which includes audio and/or video) any part of a lesson, physical or virtual, with any device unless this has been agreed with my teacher.
- I will not contact my teacher or anybody else using video or voice chat, unless for, or about, a specific task requested by my teacher.
- I will only join Team Meetings during the allocated times and will not access them before a meeting starts or after it ends.
- I will not have one to one conversation with anybody else via audio or video, except in circumstances discussed and agreed between my parents and teacher, and only then with an adult in the room with me.
- I will acknowledge and adhere to the ***'online safety rules'*** posted in classrooms around the school.
- I have read the document ***'Important Information about your use of ICT'*** and agree to follow its guidance.
- I have read and understood the school's sanctions policy for device misuse.

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

This document and related IT policies and guides are available on the school's website and Firefly and will be regularly updated in line with DfE guidance. At the start of each academic year all pupils undertake the online quiz which involves reviewing this document with their tutor or in curricular wellbeing, and finished with a sign-off agreeing to the terms of present and future amends of this document and related policies that ensure the safeguarding of the pupils.

Appendix D

IT Acceptable Use Policy for Pupils (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.

The following statements form the Pupil Acceptable Use Policy
Whether working on my home computer or at school, I understand that the Acceptable Use Policy applies to all of my online conduct when using school sites, IDs or equipment, or when representing the school in any way.

a) If using a school iPad, I understand that the school owns the iPad I use and I need to follow the rules that have been set, whether at school or at home.
b) I will only use my school iPad for school work and not for gaming.
c) I will not use a personal electronic device (such as a phone, tablet or smartwatch) at school without first receiving permission from a school manager.
d) I will only use my school email address and my own logins and passwords, not anybody else's, to access the sites I am asked to use.
e) When using Microsoft Teams, I will only use the Chat facility when required for my school work.
f) I will not contact my teacher or anybody else using video or voice chat, unless for, or about, a specific task requested by my teacher.
g) I will only join Team Meetings during the allocated times, and will not access them before a meeting starts or after it ends.
h) I will not have one to one conversations with anybody else via audio or video, except in circumstances discussed and agreed between my parents and teacher, and only then with an adult in the room with me.
i) I will not share passwords, photos, personal details or my location and I will tell an adult if anyone asks me to share them.
j) I will not write, look at or send anything inappropriate or that I would not want to share with my parents, my teachers or the Headmaster. This includes anything that is violent, racist, sexist, or intended for adults.
k) I will use appropriate language in all my work, emails and communication.
l) I will never use words that can hurt or be used to bully someone else and will tell an adult if I become aware that somebody else does so.
m) I will not record or sound or take photos unless I have permission from my teacher.

n) If I become aware of others using computers inappropriately, I will contact a teacher to report this, providing evidence if possible, so that it can be dealt with appropriately.
o) 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.

Appendix E

Pre-Prep Virtual School Acceptable Use Agreement

When using Microsoft Teams

To keep myself safe, I know that I must:

- Always follow The Caterham Way when we are learning virtually.
- Check with a grown up before opening Teams.
- Be ready to start my session on time (you will have a chance to chat to teachers after story time).
- Sit nicely just like when I am at school (ideally at a desk/table).
- Not be eating or playing with toys during a session.
- Listen carefully to the adult teaching the session and remember that we must take turns to speak and not call out.
- Not press buttons to mute or unmute microphones during sessions unless I am asked to by the teacher.
- End the video call when my teacher asks me to.

General To keep myself safe, I know that I must

- Tell a grown up if I see anything on the screen which makes me feel worried.
- Ask a grown up if I get stuck with what to click or do next.
- Not share pictures or personal information with anyone other than when my teacher is talking to me.

Appendix F

CATERHAM PREP SCHOOL

KS1 pupils e-safety agreement

Keeping me safe at home and at school

We check with a grown up before using the internet.

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

If we get stuck or lost on the internet 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, 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.

Name:

Appendix G

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 H

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 I

Online Safety Rules (for display in all classrooms)

These online safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- I understand that the school owns the computer network and the iPad I have been given and can set rules for its use. I understand it is a criminal offence to use a computer or network for a purpose not permitted by the school.
- I will only use IT systems in school, including the internet, email, digital video, iPad, etc., for school purposes. I will not use IT systems at school for private purposes, unless the headmaster has given specific permission.
- I will not use IT systems at school for personal financial gain, gambling, political activity, advertising or illegal purposes.
- I will only log on to the school network, wifi or learning platforms (such as Firefly) with my own user name and password.
- I accept that I am responsible for all activity carried out under my username.
- I will follow the school's IT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address for school-related work, and where appropriate, I will use the alias email address I have been given.
- I will make sure that all IT communications with pupils, teachers or others is responsible and sensible, particularly as emails could be forwarded to unintended readers.
- I will not send anonymous messages or chain mail.
- I will be responsible for my behaviour when using any online or digital services. This includes resources I access and the language I use.
- I will be polite and appreciate that other users might have different views to my own.
- I will contribute to public discussion spaces positively and will share my ideas constructively.
- I will not give out any personal information such as name, phone number or address through email, personal publishing, blogs, messaging or when using any of the online services you have signed up to.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher. I understand that it is against the law to take, save or send nude or semi-nude images or videos of anyone under the age of 18.
- I will not download or install software on school technologies.
- I will not attempt to bypass the internet filtering system.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I understand the school can exercise its right to monitor the use of the school's computer systems and learning platform, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

- I understand that all my use of the internet, school's learning platform and other related technologies can therefore be monitored and logged and can be made available to my teachers.

- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted. I understand that irresponsible use may result in the loss of my internet access or iPad.

Appendix J

Mobile Phone Policy

Introduction

The majority of staff and pupils own an internet-enabled mobile device which can connect by WiFi and 3/4/5G. The use of the school WiFi is explained in the staff and pupils Acceptable Use Policies, and as such, this policy explores only the 3/4/5G connectivity issues. There are 2 core reasons governing the writing of this policy: that we are an industrious and hard-working community for whom the potential interruption and disruption of 3/4/5G devices must be minimised, and that the use of unfiltered internet access brings with it many potential safeguarding concerns, as outlined in Keeping Children Safe in Education and other safeguarding documentation. As such, this policy applies to all members of our school community.
This policy applies to 'standard' mobile phones as well as smart phones such as iPhones, Android and Windows phones, and other 3/4/5G enabled devices.
This policy should be read in conjunction with:

- Online Safety Policy
- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Exclusion, Expulsion, Removal and Review Policy
- Acceptable usage Policy for pupils *and* staff
- Social Media Policy for pupils *and* staff
- Staff/Pupil Relationship Guidance

Procedures

The safe and effective running of the school is of paramount importance, however where possible a common sense approach is followed regarding the use of 3/4/5G enabled mobile devices.

- By having clear rules around the use of mobile phones, as outlined below, the School has taken steps to control and monitor the use of unfiltered internet access by its pupils. This is further reinforced through online safety education which happens through the Wellbeing curriculum, and through advice given to parents via the Caterham Online Partnership about how to monitor and regulate their children's' mobile devices when they are not provided by the school.
- Whilst some pupils may be frustrated by the School's filtering, the School aims to provide a level of filtering which is fair and useful whilst also fulfilling its safeguarding obligations, meaning that pupils will not require 3/4/5G access to complete the work which occupies much of their time during the school day.
- Through appropriate supervision and monitoring at break times, pupils are unable to access their mobile phones during the school day without explicit permission from a member of staff.
- To encourage the boarding community not to use 3/4/5G dongles on their laptops and other mobile devices, the School allows access to social media after 6pm during weekdays and at weekends via its WiFi network. This means that pupils in the boarding community have an experience similar to their peers without the need to circumvent the school's network.

- The IT Support department will monitor the presence of 3/4/5G tethering and VPNs and intervene and investigate where necessary.

Times and Locations for Permitted Use

- Staff mobile devices should be switched off or muted and in airline mode during lessons.
- The bringing of mobile phones into the prep school is discouraged but pupils sometimes bring them in to arrange pick-up times or for related arrangement-making. In these cases the phone is locked and stored in Prep Reception during the working day.
- Senior School pupils in 1st to 4th Year: mobile devices should not be used during the school day without the express permission of a member of staff. If a pupil's mobile device rings or emits an alert during a lesson it should be confiscated and given to the relevant Head of Year who will decide when to return it to the pupil and whether any other sanctions, such as a detention, should be imposed.
- Pupils in the 5th Year may be allowed to use their mobile phones in the 5th Year area at the discretion of the Head of Year.
- 6th Form pupils may use their mobile devices in the Pye Centre, but should not do so during study periods.
- 3/4/5G or WiFi enabled devices of any description, including mobile phones, iPods, smart watches or iPads must never be taken into public examinations by pupils *or* staff.

Security of Mobile Phones and other electronic devices

- The School does not accept responsibility for mobile phones or other electronic communication devices or entertainment systems. Pupils are advised to lock their devices in their lockers during the school day (Prep pupils with mobile phones will have these locked in reception during the school day). Staff should be aware that mobile phones and other such devices are not covered by the company's insurance policy. Staff are advised to keep valuables on them at all times.

Communicating using mobile devices

- If a pupil is unwell, they should report to the Health Centre who will contact their parents. Pupils should not contact their parents directly, either via phone, social media or electronic methods, to arrange to be collected.
- If parents need to contact their child in an emergency they should telephone the school office and a message will be passed on in the usual way.
- Pupils should not update social media platforms during the school day or post information about their specific location or current activity to such platforms while on schools trips. In doing so pupils could affect their personal safety or that of those they are with. Pupils and staff should refer to their relevant *Social Media Use* policy for further details and guidance on this matter.
- When directed by a teacher and within the context of an academic lesson, pupils may be given permission to use social media.

Appendix K

Remote Working Guidelines

Introduction
Remote access and working digitally form home are a normal and accepted part of working at Caterham School. There are a number of ways in which staff access and create content for work purposes and these guidelines aim to give clear parameters as to how data should be accessed and processed when not on site. All users should be aware of their own responsibilities when accessing data remotely and working off site; these responsibilities are primarily around confidentiality and data protection.

Definitions
Remote Access: accessing Caterham School systems from outside of Caterham School using any internet-enabled device. The information accessed and processed continues to reside on Caterham School systems, whether these be on site or in the cloud.
Mobile Working: carrying out work (i.e. the creation, storage, processing and transport or transfer of data/ information) as an employee of Caterham School from outside of Caterham School premises.

User responsibilities and good working practices
The primary responsibilities of employees of Caterham School and other users that remote into the Caterham School network are to:

- Know what information they are accessing, using or transferring
- Understand and adhere to contractual, ethical or other requirements attached to the information and in line with Caterham School policies and procedures.
- Users are responsible for following correct procedures when logging out of the remote session (in particular Securelink and OneDrive)

Responsibilities for data/ information accessed and/ or processed during mobile working

- Confidential data/information should not be created, stored or processed on privately owned computers, however this is permissible if you are saving directly to OneDrive and do not store copies of the data/information elsewhere
- 3rd party devices should not be considered or assumed to be secure and the use of such devices for storing documents or other work related to Caterham School is discouraged.
- Appropriate precautions and good practice should be followed for all data and information that has been edited, created and/or saved on mobile or home devices or other forms of media

Security of privately owned internet-enabled devices
If you are using a VPN to access your remote desktop (which gives you access to your PC at school) this must only be done on Caterham School provided devices.
If users are using their own personal systems or other mobile devices to carry out work for Caterham School using web-based applications such as OneDrive and iSams then the following points should be followed:

- Stay up to date with current security threats and issues for their device type, whether that is related to hardware or software, and update software appropriately and in a timely manner

- Maintain safe web-surfing practice.
- Each device should be kept up to date with anti-virus software
- Maintain good practice with use and storage of passwords
- They do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that are not relevant to their role.
- Mobile devices are not left unattended
- Data that is deemed confidential is not left visible on screens in public areas
- If a system has suffered loss of data, corruption of data or any other issues that may impact the network or other systems at Caterham School, this is reported as soon as possible to the IT Systems Manager

Security of Caterham School devices

The use of a school-provided iPad or other device provided by the school is considered secure for remote access as long as the following additional guidelines have been enacted:

- Stay up to date with current security threats and issues for their device type, whether that is related to hardware or software, and update software appropriately and in a timely manner
- The iPad has a passcode and the 'lock screen automatically' function is enabled
- Return the device to IT Support if you encounter any system faults or any other security related issues
- Maintain safe web-surfing practice.
- Avoid saving any work locally on the iPad – use OneDrive wherever possible for any work
- Passwords are kept private and not made available to other users
- iPads or other devices are not left unattended
- Data that is deemed confidential is not left visible on screens in public areas
- They do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to their role.
- School owned devices should not be used for personal IT requirements. As this could lead to downloading potential malware / unwanted files.
- These devices, should not be taken on holiday and devices should be secured whilst user is not using them.

Creating and processing data remotely

- Data created remotely in connection to work should not be shared in any ways other than through Caterham School authorised platforms, namely: the school email system, Firefly, CHIP and the 'share' feature built into office 365.
- Users should carefully consider which platform to use when sharing content remotely.
- Sensitive data (that is not related to CHIP) should only be transmitted if necessary, and with password-protection enabled on the document. Passwords for these documents must not be sent in the same email as the documents

Remote Access for Third Party Suppliers

It is often necessary for third party suppliers to require remote access to install, upgrade or troubleshoot Caterham School systems.

These instances should be undertaken only by IT Support staff. If there is any requirement for virtual technical support, you will be required to bring the device into school so that this can be successfully and safely undertaken.

Removal of Remote Access Rights

Access rights to for remote access may be changed or removed Caterham School from any user at any time if there is deemed to be a breach of the conditions of use or the user's access is compromising the confidentiality, integrity and/or availability of Caterham School's systems or services.

The remote access rights of all employees and third party users shall be removed upon termination of employment, contract, or agreement.

Appendix L

Important Information about your use of ICT

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 all of the above rules 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, you 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 who are located in the IT Workshop.

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.

BYOD

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

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

Smartphones may be used by Sixth Form pupils, but only in the Sixth Form Centre. They may not be used for sending messages or making phone calls during lesson time.

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 wifi 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

Appendix M

IT Acceptable Use Policy for the use of school laptops

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. 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.

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 hours 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 N

Caterham School AI Policy

Scope

Caterham School is committed to providing an outstanding, innovative education within a safe and secure environment and the effective and appropriate use of technology is an important part of this. With iPads and internet access available to all, it is essential that we establish clear guidelines for the use of these resources. This policy aims to outline the acceptable use of AI-enabled software, including Chat GPT as an emerging technology which will form part of their educational experience.

Acceptable Use

All staff and pupils are expected to use technology responsibly and in accordance with the school's primary Acceptable Use Policies which can be found *HERE*.

Use of AI-Enabled Software

The use of Chat GPT and other AI-enabled software is permitted within the school, subject to the following guidelines:

- Pupils may not use AI-enabled software to impersonate others or engage in any activity that may be considered deceptive or malicious.
- Pupils may not use AI-enabled software to cheat or gain an unfair advantage in any academic task. Specifically, this means not submitting AI-created content without the necessary references or acknowledgments.
- Pupils must be aware that teachers may use AI-enabled software to assist with marking. They will be informed in advance of any instances where this will occur. Teachers will always review the accuracy and integrity of AI-enabled marking.
- Neither teachers or pupils should enter any personal, or identifiable data into any AI system without clear guidance or risk assessment in place.

Pupil Training

Whilst developments in AI-enabled technologies are constantly evolving, all pupils will be given clear guidelines and training in how to make best, effective and safe use of the programs they are likely to encounter and use most often. This training will be rolled out in a number of ways, via form tutors, class teachers and both the EDGE & Wellbeing curricula. Pupils will explore both the technical use and ethical implications of AI for their school work and wider personal and social use.

Ethics Statement

As a school, we are committed to ensuring that the use of technology is ethical and responsible. With reference to AI-enabled technology this includes:

- Data Privacy: Users must respect the privacy of others and avoid storing, sharing or use of any personal information without consent.
- Bias and Discrimination: Users must be aware of potential biases in AI-enabled software and avoid perpetuating discrimination or prejudice.
- Accountability: Users must take responsibility for their actions when using AI-enabled software, and report any concerns or issues to the appropriate people within the school.

Conclusion

The use of technology, including AI-enabled software, is an integral part of education in the 21st century. Our school is committed to promoting responsible and ethical use of these

resources, and to providing a safe and secure environment for all staff and pupils. By following these guidelines, we can ensure that emerging technology is used in a way that benefits our community and promotes learning and growth.