Online Safety Policy

CATERHAM SCHOOL

CATERHAM PREPARATORY SCHOOL

ISI Code: 7h Online Safety Policy
Policy Author: Adam Webster (Deputy Head, Innovation)
Date Reviewed By Author: September 2019, with Principal Deputy Head, Deputy Head (Prep) and Head of the Pre-Prep; updated re mobile phone use March 19 (DMG)
Next Review Due: September 2020
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 has twice been 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 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.

The Online Safety policy forms part of the safeguarding policies, as well as being the over-arching 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.

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

- Safeguarding Policy
- Keeping Children Safe in Education 2019
- Wellbeing Policy
- Behaviour Policy
- Staff Acceptable Use Policy (Appendix A)
- Pupil Acceptable Use Policies (Appendix B & C)
- Staff Social Media Policy (Appendix D)
- Pupil Social Media Policy (Appendix E)
- Online Safety Rules (Appendix F)
- Mobile Phone Policy (Appendix G)
- Remote Working Policy (Appendix H)
- Important Information about your use of ICT (Appendix I)

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 Smoothwall, 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 CEOPS 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 be taken to reduce potential harm.

**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 platform (Firefly) 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 web site**

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 program 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 program, 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 2019 and its relevant additional documentation.

Parent 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.

**Managing filtering**

The School will consult Surrey County Council to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the online-safety co-ordinator (Deputy Head (Innovation)). IT Support in conjunction with the DSLs will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. The DSLs hold a log of any incidents useful in identifying patterns and behaviours of the pupils on CHIP.

Furthermore, a daily email is compiled by the school’s filtering provider (Smoothwall) and sent to the Senior Teacher (Safeguarding) and Deputy Head (Innovation) 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 email allows the DSLs to explore potential patterns and risks in a timely manner in line with our safeguarding duties, including the PREVENT duty.

**Managing videoconferencing**

Pupils should ask permission from the supervising teacher before making or answering a videoconference call (Skype, 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. Handheld technologies, including 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 Environment, Firefly 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 issued in May 2018.
POLICY DECISIONS

Authorising internet access

All staff must read and sign the Acceptable Use Policy for Staff, Trustees and Visitors 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. Secondary pupils must apply for internet access individually by agreeing to comply with the pupils’ Acceptable Use Policy, which includes internet protocols. Any person not directly employed by the school will be asked to sign the IT Acceptable Use Policy for Staff, Trustees and Visitors before being allowed to access the internet from the school site.

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. 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 to 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 fora 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 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, Trustees and Visitors

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 sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Deputy Head (Innovation) or Principal Deputy Head.

As a member of staff, trustee or visitor to the school, 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 on Firefly.
- 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 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 leave all personal mobile devices, including mobile phones and cameras, in a locked cabinet with the School Receptionist every morning, to be collected at the end of the day.
- 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 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.
- 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 3/4G 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 offense 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 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.
• The playing of games is not permitted whilst on the school site.
• I will remain signed in to 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. By digitally ‘signing’ your acceptance of this policy, you are agreeing to the terms of future versions 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.

• 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 3/4G 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 offense 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 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 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 ICT policies and guides are available on the school’s website and Firefly and will be regularly updated in line with DfE guidance. By digitally ‘signing’ your acceptance of this policy, you are agreeing to the terms of future versions of this document and related policies that ensure the Safeguarding of the pupils.
Appendix D

Staff 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 staff use social media responsibly so that they protect themselves whilst also maintaining the school's reputation.

It is crucial that pupils, parents and the public at large have confidence in schools' decisions and services. The principles set out in this policy statement are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the school are safeguarded.

This policy statement also aims to help staff use social media with minimal professional risk. Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Scope
This policy applies to all teaching and other staff, volunteers and other individuals who provide services on behalf of Caterham School. These individuals are collectively referred to as 'staff members' in this policy.

This policy covers personal use of social media as well as the use of social media for official Caterham School purposes, including sites hosted and maintained on behalf of the School.

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.

Professional Use of Social Media

- The school maintains a presence 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. Some staff have chosen to play a part in this use of social media for professional purposes, often to highlight successes and to encourage participation in their area of work. This is not without risk, however and staff members should be aware that;
services such as Twitter and Instagram are in the public domain and are regularly used by journalists, pupils, parents and employers

submissions can take on a life of their own once sent by users, who should not rely on being able to delete them

The school and parents may re-tweet/amplify the submissions of staff members to their wider following

Any members of staff wishing to make use of social media for teaching and learning purposes should consult with the Deputy Head (Innovation) in advance of creating any new accounts and details of any accounts made should be logged with the Image and Digital Content Manager and the Director of Marketing. Staff should also consult with the Image and Digital Content Manager to discuss the appropriate tone to use on social media when representing the School.

Social Media Policy Statement

Staff members must not upload video content to hosting services (such as YouTube) without sign off from the Deputy Head (Innovation). This is for reasons of safeguarding and for maintaining the reputation of the school. It is highly preferable that if using YouTube, videos are uploaded as ‘unlisted’ so that they are not public-facing. If you need assistance with this, please contact IT Support.

Staff members should maintain a professional persona through any use of social media for work purposes. User names should be formal (e.g. @MrSmith_SchoolName) or anonymised (e.g. @PE_SchoolName). The latter option also distances the user from their real life identify and makes online bullying less likely. It is also preferable as it means accounts can endure beyond the time a member of staff works at the school.

All professional submissions to social media sites must show the school in a positive light and should be written without ambiguity or any rhetorical device (such as sarcasm) which might be mis-interpreted. It is surprisingly easy for even the gentlest of humour to be read differently than intended when parsed through abbreviated media such as Twitter.

Staff members should exercise professional judgement when using social media. If in doubt over the appropriateness of a submission, the best option is not to make it. Appropriate disciplinary action will be taken should a member of staff make a submission which brings the school into disrepute.

If using social media in such a way as to engage with pupils, the staff members running those accounts are responsible for ensuring that a professional tone is maintained and that any posts or comments made by pupils are reported to the relevant Head of Year.

Any images submitted to a social media site should be chosen carefully and should show the school positively.

- Images of pupils must only be uploaded with exceptional caution; no individual or close up images should be used where the pupil’s first and surname is used. Likewise, no image which might reasonably be judged to cause embarrassment to the pupil should be published. ‘Over the shoulder’ images (where individuals are not recognisable) or group shots of 3 or more pupils are safest.
Images of individual staff should only be uploaded with their consent and no image which might reasonably be judged to cause embarrassment to the member of staff should be published.

Individual pupils should not be identifiable through submissions to social media sites, for safeguarding reasons. For example, “Excellent piece of Level 7 work shown here by Tom in Y8” is acceptable, whereas including Tom’s surname is not. Any submission that includes an image of a pupil must not make reference to the pupil’s sur- or full name under any circumstances.

- 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. The potential for hi-jacked accounts to bring the school into disrepute is significant and responsibility for account security lies with the staff member who controls it. Staff should be cognisant that such accounts are likely to be targeted by pupils for precisely this purpose.

**Personal Use of Social Media**

It is reasonable for members of staff to maintain personal web presences in their lives beyond their school life. School staff, however, occupy an almost unique professional position due to their work with children and the moral credibility they must maintain.

It is worth considering that information (text, images, video) held in web presences:
- 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**

Staff members are advised not identify themselves as employees of the school in their personal web presences or purport to represent the views of the organisation. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

Staff members must not have contact through any personal social media with any pupil or member of a pupil’s family, whether from their school or any other school, unless the pupils are family members. Even being linked to the children of colleagues/ close personal friends carries risks, as many services such as Facebook allow user data to be visible to friends-of-friends. For example, that photograph of Friday night at the end of term could, once commented on or liked by one of your direct contacts, be visible by multiple third parties over whom you have no control.

Staff members should be aware that if they maintain an extreme political, religious or philosophical views expressed via social media that conflicts with those of the school they may find that their position at school to be untenable.

Staff members should not use social media to document or distribute evidence of activities in their private lives that may bring the school into disrepute. Even if separation of professional and private
lives has been maintained, recent case history shows that teachers whose behaviour becomes known through social media have found their position at school to be compromised.

Staff members must decline ‘friend requests’ from pupils they receive to their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they should discuss these in general terms in class and signpost pupils to become ‘friends’ of the official school Facebook, Instagram or Twitter accounts.

On leaving the school’s service, staff members must not initiate contact with former pupils by means of personal social media sites whilst that pupil is under the age of 18.

Staff members must not initiate contact with former pupils by means of personal social media sites whilst that pupil is under the age of 18 or in full time secondary or 16 to 19 education. If the former pupil has family and/or social media friends in the school, they should continue to refrain from initiating contact with former pupils by means of personal social media sites.

Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues and other parties must not be discussed on their personal web presence.

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.

Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity from work. This is because the source of the edit will be recorded as the employer’s IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Staff members must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or the school.

Staff members 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 E

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 Sullivan.
• 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 F

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 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 G

Mobile Phone Policy

Introduction

The majority of staff and pupils own an internet-enabled mobile device which can connect by WiFi and 3/4G. The use of the school WiFi is explained in the staff and pupils Acceptable Use Policies, and as such, this policy explores only the 3/4G 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 3/4G 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 2019 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 3/4G enabled devices.

This policy should be read in conjunction with:

- Online Safety 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 3/4G 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 3/4G 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 3/4G 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 3/4G 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.
- 3G, 4G or WiFi enabled devices of any description, including mobile phones, iPods 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. 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 H

Remote Working Policy

Introduction
Remote access and working digitally from 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 users are using their own personal systems or other mobile devices to carry out work for Caterham School 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
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 your 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
- 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 your role.

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
In these instances remote access should be monitored until the completion of the installation and the remote session has ended.
Third party suppliers remotely accessing Caterham School systems must contact the school and inform them of any changes that are to be made along with times and dates of the required remote access session.
User accounts for third party suppliers and support should be kept disabled when not in use.
Removal of Remote Access Rights
Access rights to 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.
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