Online Safety Policy

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

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.

Safety policies, training, curriculum opportunities, procurement decisions and monitoring strategies.

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

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

Appendix A

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

- 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 offenc**e 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

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 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.**
-

Appendix D

IT Acceptable Use Policy for Pupils (Prep School)

n)

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.

Appendix F

CATERHAM
PREP
the internet.
not share on
We will not bring mobile phones or other electronic

Appendix G

- 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 hi**gh 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.

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**

- 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 pri**vate 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

- 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 communicatio**ns 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

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

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 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

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

‡

- 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

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

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:

Removal of Remote Access Rights

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.

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.

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.