The School prides itself on its innovative approach to the use of technology in line with its ethos and aims, and is recognised as an industry leader in this field. Caterham School remains recognised as an

consensually), viewing and sharing pornography, grooming, enticing children to engage in extremism or sexual behaviour and face to face meetings.

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

**: making sure our boarding pupils are safe online and not accessing or exposed to inappropriate material is essential. While our web filters have a significant role to play here, this alone does not prevent the possibility of boarders using the mobile networks listed above to access inappropriate content, nor from their bringing inappropriate content to school already downloaded onto a device. In caring for our boarders, the School seeks to balance our duty of care to keep them safe with their rights to privacy and a homely environment. We adopt a profiled approach to mobile devices, which sees pupils up to Y10 inclusive hand their devices in at bedtime, while our Y11, 12 and 13 are trusted to hold theirs and behave responsibly. However, any online/mobile phone concerns about individual pupils in these older years sees their devices handed in for an appropriate period of time. We promote (as indeed we do with all pupils)
if they are aware of inappropriate content on a device, and ally this with assemblies and Wellbeing**

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

The use of technology, including AI-enabled software, is an integral part of education in the 21st century. Our school is committed to promoting responsible and ethical use of these resources to ensure that emerging technology is used in a way that benefits our community and promotes learning and growth. The use of Chat GPT and other AI-enabled software is permitted in accordance with agreed guidelines (see Appendix M).

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

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

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

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.

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.

The School's policy on social networking is robust:

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

Pupils are advised never to give out personal details of any kind which may identify them or their location. Further guidance on this matter are explored in the pupil *Acceptable Use Policy* and the pupil *Social Media Policy* found in the appendix of this document. Much time is spent educating pupils about the benefits and risks of the internet and social media through the Wellbeing curriculum, details of which can be found in the school's *Wellbeing Policy*. This guidance is informed by the School's own experiences with social media and by Keeping Children Safe in Education 2024 and its relevant additional documentation.

Parents and pupils are offered guidance on the safe use of social media through My School Portal. 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.

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

A daily report is compiled by the School's filtering provider Smoothwall and sent to the DSL, Deputy Head (Innovation), Deputy Head/ DSL (Prep School), Assistant Head (Boarding) Head of Wellbeing, DDSL (Assistant Head First Year)which lists all searches made by the school community which reach a safeguarding threshold.   This report allows the DSL to explore potential patterns and risks in a timely manner in line with our safeguarding duties, including the PREVENT duty. A record of concerns and outcomes is maintained by the DSL.

Between the hours of 8am – 6pm Monday to Friday during term time the safeguarding team will be notified of concerning behaviour in real time, which is logged and followed up as appropriate. Filtering and monitoring software continues to operate on iPads whether they are on or offsite, and at all times of the day. Concerning behaviour on school devices outside the hours of 8am -6pm will

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

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

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 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 tutor sessions.

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

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

Parents should be given access to online safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust. The School performs this duty through parent webinars and via My School Portal.

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.

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

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

I appreciate that IT includes a wide range of systems, including my iPad, mobile phones, PDAs, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.

I understand that it may be a criminal offence to use a school IT system for a purpose not permitted by its owner.

I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.

I understand that I am responsible for all activity carried out under my username.

I will only use the school's email, internet, learning platforms such as Firefly and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headmaster or Board of Trustees.

I will only use the approved, secure email system for any school business.

I will ensure that personal data (such as data held on iSAMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Hard copies of sensitive personal data should only be taken out of school when authorised by the Headmaster or Board of Trustees. Sensitive personal data should not be transferred to external hard drives, including USB sticks.

When working away from the school site, I will refer to the guidelines given in the Remote Working policy, which can be found in Appendix K of this document .

I understand the importance of protecting and monitoring my use of data in line with GDPR regulations. In particular, I will adhere to the school's policy on the creation and retention of personal data and will refer to the school's Privacy Notice, the GDPR working party or the Principal Deputy Head should I be unsure of what data I can hold.

I will not install any hardware or software without the permission of the Deputy Head (Innovation) or IT Systems Manager.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I understand that my use of the internet and email, when accessed through the School network

Images and audio recordings of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and (where appropriate) with written consent of the parent, carer or staff member. Images and audio recordings will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Headmaster.

I will ensure that my online activity will not bring the School into disrepute.

I have read the *Staff Social Media Policy* and I understand and agree to its content.

I will strive to ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

All EYFS staff will ensure that personal mobile devices, including mobile phones and cameras, are kept out of sight and reach of pupils.

I will support the school's Online Safety Policy and help pupils to be safe and responsible in their use of IT and related technologies. I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

I will ensure that I have understood the protocols around video conferencing pupils, and in particular, in conducting 1-to-1 meetings with pupils, in line with our Safeguarding Policy

I will report any incidents of concern regarding children's safety to the DSLs or the Headmaster.

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.

- 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 or offensive 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 respect the laws of copyright and ensure that sources used are referenced.
- I will not use AI to produce work without my teacher's permission and will reference my use of AI in my finished work.
- 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 use my device as directed by my teachers and will do nothing to bring the school into disrepute.
- I will only use my school email address for school-related work, and where appropriate, I will use the alias email address I have been given.
- I will not send anonymous messages or chain mail.
- I will not attempt to circumvent the school's filtering in any way, including, but not limited to using a 3/4/5G connection, including tethering the device to my phone, nor by using a proxy server, or VPN. Nor will I adjust or alter any profiles, software or hardware, including jailbreaking the device.
- I will only be connected to the 'Caterham Wifi' network.
- First to Fifth year pupils should not have any other devices connected to the network unless permission has been granted from the SENDCO or their Head of Year.
- I understand that viewing/reading/modifying/storing/editing any HTTP or HTTPS internet traffic, or any other attempts to retrieve personal data that has been stored digitally is totally unacceptable.
- I will only ever use my own account (Please note that sharing your logon details with others will be dealt with as an equally serious offence as using another person's account).
- I will not attempt to modify static IT equipment.
- I understand that torrenting, peer to peer networks or illegal file sharing are not permitted
- Social media may only be used at the discretion of my teacher in consultation with the Senior Management Team.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher.
- Profiles created for school-based accounts will use the anonymized (numerical) emails given to me. I will not use real photographs of myself or other pupils as an avatar, and where possible I will give reduced personal information such as my first name and first initial of my surname. I should speak to a member of staff about creating these accounts if I am unsure.
- I understand the behaviour expected when meeting with teachers and pupils virtually for the purposes of learning
- When using Microsoft Teams, I will only use the Chat facility when required for my schoolwork.
- I will not record (which includes audio and/or video) any part of a lesson, physical or virtual, with any device unless this has been agreed with my teacher.
- I will not contact my teacher or anybody else using video or voice chat, unless for, or about, a specific task requested by my teacher.
- I will only join Team Meetings during the allocated times and will not access them before a meeting starts or after it ends.
- I will not have one to one conversation with anybody else via audio or video, except in circumstances discussed and agreed between my parents and teacher, and only then with an adult in the room with me.
- The playing of online games is not permitted whilst on the school site.
- I will remain signed into my school-given iCloud account (ending @appleid.caterhamschool.co.uk) at all times.
- I will acknowledge and adhere to the 'online safety rules' posted in classrooms around the school.
- I have read the document 'Important Information about your use of ICT' and agree to follow its guidance.
- I have read and understood the school's sanctions policy for device misuse.

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

This document and related IT policies and guides are available on the school's website

---

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. E1 0 0 0.1 0 0 cm   0 g   q   10 0 0 10 0 0 cmf

- **I will not share content that puts me, or anyone else at risk in any way, this includes**

- 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.

One-to-one audio or video conversations are restricted and require parental and teacher agreement.

My passwords, photos, personal details, or location will remain confidential. I will notify an adult if someone requests such information.

Everything I view, write or send will be appropriate and not harmful. I will not view, create or share violent, racist, sexist, homophobic or age-inappropriate content.

I will use polite language in all online interactions and notify an adult immediately if I observe unkindness or bullying.

Recording video, audio or taking photos requires teacher permission.

I will report any inappropriate tech use to a teacher because this will help to keep everyone safer.

I understand that if I do not behave appropriately, the school may not allow me to use the computer and/or iPad and my parents may be contacted.

I will only use generative AI tools under adult supervision.

I will not share personal information about myself or others when using generative AI.

However, some inexperienced social media users sometimes think, incorrectly, that online activities, whether on open or closed networks, operate outside normal expectations and laws of engagement. There are risks associated with the use of social media which can impact on the safety, health, and wellbeing of individuals and also on the reputation of the school. Additionally, misuse of social media can amount to unlawful activity and/or contravene school policies. The law of defamation applies to social media activity just as it

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

disclaimer, such as: "The views expressed here are my own and do not necessarily reflect the views of Caterham School."

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

4.

Caterham School's policy framework commits to ensuring a safe and welcoming environment in which all pupils and staff thrive and achieve their full potential. It expects all staff, volunteers and pupilsupilsj   ( )'   T[.()-4(a)3.008-4.003(t)-2.926( )-4(ie)11.905( )-4nliwith ( )'412(t)-2.92(

)-2.98542(c)3.00532(oo)8.98942(t)-2.99426(ne)11.9903(t)-2.99426( )6.01285(whi)2.9832(c)3.00532(h)-3.99382damCage

ScEoo   l'   r   t   ioEs   wi

•

exercised in accordance with the law. To do so could stray into behaviour that amounts to bullying, harassment or intimidation It may also be a breach of the civil or criminal law.

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

There are a raft of legal issues relating to social media ranging from defamation, where untrue content affecting a person's or organisation's reputation is posted, which causes, or is likely to cause, harm. Harassment, where someone is subjected to conduct, causing distress

4.5.2

All School social media accounts must adhere to the School's brand guidelines and give clear indication of their purpose. If several members of staff run the same social media account, a

- **ensure the social media account is the original rights-holder of the content you want to share – and if they aren't, ask who is and contact them directly to seek permission**
- **ask the social media account permission to share their content on the platforms you're planning to use and include a credit line, unless you're sharing directly on the platform you found the content, such as a retweet.**
It's especially important not to publish content or contact details of staff or pupils without their express permission. Pupils' consent to be photographically featured can be found on iSams. Before taking a school trip or activity it is strongly recommended that all pupil participants' photo consent is checked prior to the trip taking place.

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

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 with my own user name and password.
- I accept that I am responsible for all activity carried out under my username.
- I will follow the school's IT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address for school-related work, and where appropriate, I will use the alias email address I have been given.
- I will make sure that all IT communications with pupils, teachers or others is responsible and sensible, particularly as emails could be forwarded to unintended readers.
- I will not send anonymous messages or chain mail.
- I will be responsible for my behaviour when using any online or digital services. This includes resources I access and the language I use.
- I will be polite and appreciate that other users might have different views to my own.
- I will contribute to public discussion spaces positively and will share my ideas constructively.
- I will not give out any personal information such as name, phone number or address through email, personal publishing, blogs, messaging or when using any of the online services you have signed up to.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher. I understand that it is against the law to take, save or send

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.

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

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.

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)

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

Access rights to for remote access may be changed or removed Caterham School from any user at any time if there is deemed to be a breach of the conditions of use or the user's access is compromising the confidentiality, integrity and/or availability of Caterham School's systems or services.
The remote access rights of all employees and third party users shall be removed upon termination of employment, contract, or agreement.

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.

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 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.**

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

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

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

Pupil Name: …………………………………………………………………

Pupil Signature: …………………………………………………………………

Parent/Guardian Name: …………………………………………………………

Parent/Guardian Signature: …………………………………………………………

Date: ……………………………………………

Pupils may not use AI-enabled software to cheat or gain an unfair advantage in any academic task. Specifically, this means not submitting AI-created content without the necessary references or acknowledgments.

Pupils must be aware that teachers may use AI-enabled software to assist with marking. They will be informed in advance of any instances where this will occur. Teachers will always review the accuracy and integrity of AI-enabled marking.

Neither teachers or pupils should enter any personal, or identifiable data into any AI system without clear guidance or risk assessment in place.

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