CLAREMONT
FAN COURT SCHOOL

POLICY:

TECHNOLOGY ACCEPTABLE USAGE FOR PUPILS AND PARENTS

This policy should be read alongside the Online Learning Responsible User Agreement (Appendix A).

Policy consultation and review

This policy is available on our school website and on request from the school office. We also inform parents and carers about this policy when their children join our school.

Policy statement:

This policy applies to the use of computers, laptops, mobile phones, tablets, digital cameras and any other electronic devices. The advice given also applies to their use outside school since our aim is to teach pupils to use technology safely at all times.

At Claremont we believe that computers are essential tools used to support learning and teaching. We also recognise that other electronic devices such as mobile phones and tablets play an increasingly important role in the life of the pupil. With these tools comes a responsibility that must be accepted by our school community. Our school network provides access to shared resources such as printing, file storage, email and the internet, which offers vast, diverse, and unique educational resources. This worldwide access is accompanied by additional responsibilities. The users' behaviours and actions now represent the Claremont community in a global arena.

Although the internet provides a unique opportunity for learning, its nature also makes materials available that have no educational value and some that many may find inaccurate and offensive. Though the school endeavours to protect our pupils from such sites and reserves the right to supervise our pupils, Claremont cannot guarantee that every objectionable site will be blocked in advance or that every student will be monitored at every moment.

1. Computer technology and internet safety

The following paragraphs refer to the use of laptops or any other electronic device, whether purchased via the school or brought in.

To permit your child to use laptops or any other electronic device on the school network and internet, both you and your child must adhere to the following guidelines. Breaches of these guidelines may result in disciplinary proceedings and/or notifying the appropriate law enforcement agency. Where the term 'generating' is used, this refers to the use of generative AI and similar tools.

The following uses of the Claremont network and internet access are <u>NOT</u> permitted:

1. Accessing, uploading, downloading, generating or distributing pornographic, sexually explicit, extremist, terrorist or otherwise obscene material or material of an excessively violent or hateful nature. If a suspected criminal act has been committed, the school is legally required to contact the police without informing parents.
2. Transmitting or generating obscene, abusive, or sexually explicit language.
3. Accessing another person's information without their permission.
4. Sharing or the creation of self-generated intimate images or videos including deepfakes.
5. Processing, altering or generating through AI, the image, photograph or likeness of any staff member or student.
6. Violating copyright or otherwise using the intellectual property of another individual or organisation without permission. This similarly applies to the misuse of AI tools and AI chat bots in relation to intellectual property and copyright restrictions.

7. Attempting to circumvent access to school software, network filters or security systems.
8. Accessing music/games/portable apps in school, except with permission from a member of staff.
9. Identifying yourself as someone other than who you are (or being anonymous) by the use of screen names or any other means of disguising or changing identity.
10. Passing off the work of other people as your own. This includes submitting or passing off AI generated content as your own without appropriate or stipulated disclosure.
11. Using the network or accessing the internet for financial gain or commercial activity.
12. Using the network or accessing the internet for dating purposes or gambling.
13. Installing any software onto a device connected to the school network, without permission from a member of the IT department.
14. Personal electronic devices will only be connected to the school network with permission from the IT department and only if the device has an up-to-date anti-virus program.
15. The use of social networks or applications such as *Facebook* or *Instagram* are not permitted during school hours, unless approval has been given by a member of staff for an authorised educational or school related purpose.
16. Cameras or mobile phones (or other "smart" devices) are not permitted to be used in the toilets or changing areas and are not to be used in a manner that may offend or cause upset to any member of the school community.

The following rules of technology usage, security and personal responsibility are to be observed at all times:

1. Adhere to the same standards of behaviour online that you follow offline. Be polite. Abusive, derogatory language or cyber-bullying is not permitted or tolerated. AI enabled harms constitute part of your online behaviour.
2. Any personal information such as your full name, address or telephone number should not be given out without your parents' or teacher's permission.
3. Do not give out your passwords to anyone.
4. Never agree to meet with someone you met online without your parents' permission.
5. Any information or experience that makes you feel uncomfortable should be reported to your teachers, parents or the IT department.

Accounts and passwords

Passwords protect the school's network and computer systems. It is the pupil's responsibility to choose a secure and strong password. This should not be the same as your widely used personal passwords.

You must not let anyone else know your password, nor keep a list of passwords where they may be easily accessed and must change it immediately if it appears to be compromised. You should never use a computer whilst it is logged in to another user's account.

You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Filtering and monitoring and keeping the school network safe

The school adheres to best practice regarding teaching and the internet. The school has appropriate filters and monitoring systems (Smoothwall) in place to safeguard pupils and staff from potentially harmful and inappropriate material, including terrorist and extremist material, online when using the school's IT system. Certain categories of websites are blocked by the school's filtering system and the IT department and designated safeguarding lead monitor email and internet traffic for both staff and pupils.

The school ensures compliance with the DfE's 'filtering and monitoring standards for schools' by:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing the filtering and monitoring provision at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet our safeguarding needs.

In terms of filtering, the school utilises a firewall service (Smoothwall) to filter content and thus ensure that all pupils and staff using the Claremont Wi-Fi networks are prevented from being able to access, generate or receive material that is not suitable for a place of education and/or work. For devices issued or managed by the school (including all pupil laptops from Year 3 to Year 11) this filtering operates whether the devices are on or off the school premises.

For monitoring, Claremont uses the Smoothwall platform to ensure that pupil devices are monitored 24/7 (including when off-site) for any inappropriate and/or concerning use of language and/or attempts to access content which is inappropriate (balanced alongside access for educational need). Smoothwall monitoring and safeguarding software triage alerts according to their severity, which includes an email alert service at 'L4' and a phone call to the DSL for 'L5'. Claremont also uses Sophos as an internet security software (like anti-virus) which blocks bad applications; this is monitored by the IT team. The DSL is ultimately responsible for all elements of the above and meets regularly with the IT department to ensure the systems are working as expected. These systems are reviewed on an annual basis.

At sixth form level, the school operates a BYOD (bring your own device) policy. When used on site these devices are monitored exactly as above. When off-site (e.g. on a home Wi-Fi network) they are not monitored. Parents of sixth-form pupils are therefore strongly recommended to make use of the parental control tools provided by broadband services (such as BT, Sky).

Upon request of the school, a pupil must provide access to their laptop. The school reserves the right to review any information stored on a pupil's laptop or device including any removable media they have with them at school. This will only be requested when an aspect of the technology acceptable usage policy is suspected of having been violated. At other times we respect the individual's right to keep their data confidential, in accordance with current data protection laws.

Laptops

Pupils with laptops must adhere to the following:

1. Pupils must bring their laptops to all classes, unless a teacher specifies otherwise. It is the pupil's responsibility to ensure that their laptop is fully functional at all times, and, if not, to report the problem to the IT department at their earliest opportunity.
2. When a laptop is not in the pupil's possession, it must be locked in a designated secure location and never be left unattended in any part of the site.
3. Laptops must be kept in the approved case at all times and named.
4. Only the supplied power adaptor may be used with school scheme laptops. Replacement chargers may only be purchased via the school.
5. Laptops are to be charged at home to avoid the disruption caused to lessons of laptops running out of battery power.
6. Damaged or faulty laptops or chargers must be reported to the IT department immediately and not used as they could be potentially hazardous.
7. Do not store paper in the protective case or underneath the laptop as this reduces the air flow and risks the laptop overheating and failing.

Laptop identification

It is mandatory that each laptop and case exhibit the pupil's name clearly. Luggage tags are recommended. Personal laptops bought independently of the school's laptop scheme (sixth form only) are solely the responsibility of the owner.

Laptop maintenance

Each pupil involved in the Claremont laptop scheme is responsible for the general maintenance of their laptop. Should a problem arise, pupils are advised to seek assistance from other pupils first, their teachers second and finally from the IT department.

Procedure if laptop is missing

If a laptop cannot be found during a pupil's day in school, they must report the matter to a member of staff and the IT department. If the laptop goes missing from outside the school premises or theft is suspected the parents of the pupil must report this theft to the police immediately. The suspected theft or loss must then be reported to the IT department.

2. Electronic devices and their safe and responsible usage

The school recognises the need for pupils of a certain age to come to school with an electronic device such as a mobile phone. The school has specific rules and guidelines to ensure appropriate and safe use of such devices.

Through pastoral sessions and the PSHE programme, pupils are taught how to positively use devices and the dangers of using them incorrectly or inappropriately. They are taught how to avoid becoming a cyber-bully or a victim of such practice, as well as avoiding plagiarism and adhering to copyright regulations.

The school educates pupils on the damaging consequences of sending inappropriate images of themselves, often referred to as 'sexting', and explains the consequences of posting offensive comments online, or images of themselves or others and how these can affect

their future prospects. Pupils are taught to value themselves and not to compare their image to online friends, peers and other persons online. Pupils are also educated on the dangers of online strangers and to never arrange to meet in person someone they have met online or to share their personal information.

Staff are trained in measures to prevent pupils from being drawn into terrorism and how to challenge the extremist ideology that can be associated with it. Staff can obtain support for pupils who may be being exploited by radicalising influences.

The school recognises the vital role parents play in educating their children to use the internet safely and responsibly. The school has an internet safety webpage (under the Parent Area) and takes the opportunity to promote internet safety via parent events. The school encourages parents to talk with their children about what they are doing, who they are talking with and where they are going on the internet and to use technology in a supervised central family area at home.

Each school within Claremont has a specific policy on the use of mobile phones, cameras and other smart and electronic devices.

Junior school (Fan Court) (Pre Nursery to Year 2)

Mobile phones, cameras, smart watches and all other smart or portable electronic devices are not to be brought into school by children under any circumstances. If a child is found with such a device, it will be confiscated and stored in the school office until the end of the day.

For pupils age 2-5, screen time will be limited to no more than 1 hour per day and less wherever possible. Further information can be found in the Early Years Foundation Stage Policy.

Junior school (Stable Court) (Year 3 to 6)

Home contact by pupils during the day is always through a member of staff and usually via the school office. Mobile phones, cameras, smart watches, and all other smart or portable electronic devices are not allowed to be brought into school by children, except for the school-approved laptop. The only exception is a mobile phone for those children who take the school bus home. Permission should be sought in writing from the head of the junior school in the first instance. If permission is granted, mobile phones must be handed in to the school office at the beginning of the school day where they will be kept securely until collection at the end of the day. If a pupil is found with a mobile phone, it will be confiscated and stored in the school office until the end of the day; there may be disciplinary consequences as deemed appropriate.

Mobile phones are not to be used by junior school pupils during the school day, including during excursions and at all times on residential trips or camps. If needed for home transport arrangements, they may be used to call parents/guardians after school or at the conclusion of the activity/excursion. No social or unauthorised calls are to be made by preparatory school children at any time whilst they are on school premises or on official school activities. We request that parents do not contact children on their mobile phones during the school day. All communication should go via the school office or teacher.

Cameras may be used on school trips at the discretion of the trip organiser. Any images taken on school trips must not be uploaded to any social media site.

The use of electronic tracking devices, such as Apple AirTags, is becoming more common, particularly to monitor children's journeys between home and school. While these devices are usually used with the intention of keeping children safe, there could be situations in which their use may raise safeguarding concerns, for example, when there is a family court order or restrictions on parental contact. If this is a concern for an individual case regarding a pupil using a tracking device, the matter will be referred to the Designated Safeguarding Lead (DSL) for further consideration.

Senior school (Years 7 to 11)

Cameras and all other portable electronic devices (excluding mobile phones and the school approved laptop) are not to be brought into school except in exceptional circumstances e.g. when a camera is needed for a photography project. In these circumstances, pupils must seek permission from their subject teacher in advance, and the equipment is only to be used for the specific purpose of the project and is to be stored securely when not in use.

Mobile phones are allowed to be brought onto the school site but for pupils in Y7-11 they must be turned off and secured in Yondr pouches during the school day, i.e. between the hours of 8.25am and 4.00pm apart from Year 12 and 13 who may use them but must not use the camera function. Unauthorised use of mobile phones will result in the phones being confiscated. The school takes no responsibility for the loss of mobile phones or any other electrical equipment and accessories brought onto site by pupils. It is strongly recommended that pupils own a basic model mobile telephone for school purposes thus avoiding issues that can be associated with smart technology phones. Mobile phones must be permanently named.

Sixth form (Year 12 to 13)

Cameras, laptops and other smart or portable devices can be brought into school by sixth form students for the sole purpose of a study aid or tool, for example using the device to take notes or to access their school emails.

Mobile phones are allowed to be brought into school by sixth form students who may use them in or just outside of the sixth form centre only, but any images taken must not be uploaded to any social media site. Unauthorised use of mobile phones will result in the phones being confiscated. The school takes no responsibility for the loss of mobile phones or any other electrical equipment and accessories.

Recording of internet safety incidents

The school maintains records of all internet safety incidents via Smoothwall. Any such incident is reported to the relevant designated safeguarding lead (DSL). Offsite instances using other technologies are more difficult to track, but without going beyond its legal parameters, the school will act upon all information provided where appropriate.

Treating others with respect

Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The school's anti-bullying policy is set out in each school's parent information booklet, in accordance with our mission and values. Claremont is committed to promoting equal opportunities for all.

All pupils are encouraged to look after each other and report any concerns about the misuse of technology or a worrying issue to a member of staff. The misuse of technology will always be taken seriously and may be the subject of disciplinary procedures.

3. Taking, storing and using images (photographs and videos) of children

At Claremont, we enjoy celebrating the achievements, experiences and everyday moments that make school life so special. Photographs and videos help us share learning, recognise success, keep families informed about school events and give current and prospective families a genuine insight into life at Claremont.

We regularly use images to reflect the progress of our pupils and the wider school community, and to communicate the vibrant opportunities and experiences available here. We use images carefully, respectfully and in accordance with UK data protection law. We take

data protection and cyber security very seriously and have appropriate measures in place to ensure that personal information is handled securely and responsibly.

We are also aware that parents and pupils really enjoy being able to see their images and would like to give all pupils this opportunity.

The school seeks consent from parents/guardians to the use of a child's image when they join the school. Consent can be withdrawn at any time in writing (see below).

There are a number of instances when the school may take photos of pupils; specifically:

- We publish photos on the school's website to promote the school to current and prospective parents, as well as providing updates on current events; we take steps to restrict copying or downloading of images;
- We publish photos and videos on our social media accounts - such as Facebook, TikTok and Instagram to provide updates on events and news within the school.
- From time to time, we publish videos via our YouTube channel and through Vimeo, which we use to host and share video links; these videos may be viewable by subscribers or via shared links;
- Within our newsletters, we may provide photos of recent events or achievements from our pupils;
- In order to promote the school, we send out prospectuses, flyers, leaflets and brochures which contain images to show life at our school. These will be sent to prospective parents;
- We may also use other promotional materials such as banners and signs which may contain photographic images for prospective parents to view;
- We publish photos in and around the school building to illustrate to current pupils and parents' life around the school including educational materials and images of recent trips and events. These can be seen from time to time by other parents or visitors within the school;
- In promotional materials to show the history and character of the school to future generations.

The school follows guidance as set by data protection legislation (mainly the UK General Data Protection Regulation) as well as guidance set by the Information Commissioner's Office on taking photos in schools and obtaining consent.

Pupils will only be named in photographs using their first name and year group.

Consent to using a child's images will last throughout their time at the school and will continue to apply for a short time after they leave (except for images published for historical purposes which may be kept for an extended period of time to show the history of the school).

The school respects parents' and pupils' wishes and will respect their decisions when publishing photographs. Consent can be withdrawn at any time by contacting the admissions and marketing team, asking for the school to stop using your child's images (imageconsent@claremont.surrey.sch.uk). At that point they will not be used in future publications, but we cannot prevent them from continuing to appear in publications already in circulation.

From time to time, the school may be visited by the media who may take photographs or film footage at a school event. Pupils may then appear in local or national media.

Fair processing

We seek consent from parents/guardians for the use of a child's image when they join the school. Consent can be amended or withdrawn at any time by contacting the school via email imageconsent@claremont.surrey.sch.uk.

The school's use of images

Claremont may use photographic images of its pupils (unless a parent has refused consent) for the following purposes:

1. Internal displays on digital and conventional noticeboards within the school premises.
2. Communications with the school community (parents, pupils, staff, Governors and alumni) via the school's official platforms such as newsletters and the school's website.
3. Marketing the school digitally through the website, the school's own authorised social media accounts, the school prospectus, local press, displays at educational fairs and other marketing functions within the UK.

Images that the school uses for displays and communications purposes never identify an individual pupil by their full name. The school only uses images of school activities, such as plays, sporting fixtures and school trips in their proper context. The school will never use any image that might embarrass or humiliate a pupil and only when suitably dressed. Pupils are always supervised when professional photographers visit the school.

The school prohibits the use of any pupil images on any external website or platform other than its own official school platforms, without express permission. This also prohibits the use of images being processed by external AI tools.

Use of images for internal identification

All pupils are photographed on entering the school and thereafter annually for the purposes of internal identification and safeguarding. They are securely stored in the school database where access is restricted to academic, pastoral and administrative staff.

Storage and review

Photographic images are stored securely on the network or in the secure school database. Parents are advised that the school will endeavour not to use images of their children in any new school material once they have left the school. Please note that the school's existing publications, website and archived material may contain these images.

Media coverage

Claremont will endeavour to notify parents in advance when it expects the press to attend an event in which its pupils are participating, and it will make every effort to ensure that children whose parents or guardians have refused permission for images of their children to be used are not photographed by the press.

The media operate under their own professional standards, including the Editors' Code of Practice. The school will consider making a complaint to IPSO if it believes those standards have not been followed. Photographs taken for journalistic purposes may be subject to specific exemptions under data protection legislation, although such photographs are not automatically exempt from the law.

Use of cameras and recording equipment by all school staff including EYFS

The following guidelines must be adhered to by school staff when using cameras, recording equipment and pupil images:

1. Images should only be taken and edited on school issued equipment and not on staff personal cameras, phones or other devices. In an unavoidable situation where a staff member has used their personal device, the image must be downloaded to the school network at the earliest opportunity and deleted from their personal device.
2. Staff members should be sensitive to any pupils who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.
3. All photographs taken of pupils should have context. Staff should avoid one-to-one situations with no surrounding context.
4. All pupils must be appropriately dressed.
5. The use of cameras is prohibited in toilets and changing areas (including backstage).
6. All images will be stored securely and used only by those authorised to do so. All images not retained for further use must be deleted.

CCTV

Claremont believes that closed circuit television (CCTV) cameras offer improved security protection for both pupils and staff. Claremont informs parents that it has CCTV installed on its premises for the sole purpose of surveillance for security and safeguarding reasons. Notices are clearly displayed in areas around the school. It is not installed in changing rooms or toilets.

Claremont is registered with the Information Commissioner's Office and has an appointed member of the school's management team who oversees all aspects of the use of surveillance CCTV within the school. Parents are assured that Claremont does not stream images collected via CCTV to any third parties or outside agencies. Please note that the school may be legally required to provide CCTV footage to the police or other law enforcement agencies if requested.

Taking, storing and using images of children (including on mobile phones) across the school by parents and carers

Current data protection laws cover the fair processing of data and images that must be adhered to. This can affect the images that parents may take at events.

Parents, guardians and visitors, attend events at the invitation of the school. The head of school has the responsibility to decide the conditions that will apply; to keep all children safe

and to ensure the performance is not disrupted for other members of the audience and the children are not distracted.

The school does not allow photography or recording during any school events. Opportunities may be offered by a senior member of staff at the end of an event. If so, parents may take photographs of their own child only.

If photography and recording are permitted by the head of school, then parents and visitors will continue to be prohibited from:

1. Taking photographs or videos of their own child or any other child in the swimming pool, changing rooms or backstage changing area.
2. Taking photographs or videos of any child during gymnastics events.
3. Using flash photography, as it can disturb others in the audience and those performing. It can also cause distress for those with medical conditions.
4. Selling or uploading any pictures or videos to any social media sites such as Twitter, Facebook and YouTube. To do so would infringe the rights of other parents and children. Parents must use photographs and videos taken at school events for personal use only.
5. If you are accompanied or represented by people that staff do not recognise, the school may need to check who they are, if they are using a camera.

Copyright

Parents are reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts. The school always prints a reminder in the programme of events where issues of copyright apply.

Professional recordings

Claremont may record major plays and concerts professionally, provided the relevant consent has been obtained. Copies may be available for parents to purchase.

Appendix A

Guidance for Remote Online Home Learning

Responsible User Agreement for Pupils

During periods of remote online home learning, by logging on to Teams, or other online platforms recommended by the school, pupils will be required to agree to and abide by the following rules:

- I will only use technology for school purposes as directed by my teachers
- I will only use technology when there is an adult in the house and they know I am using it
- I will not reveal any personal information, such as my full name, address or phone number, or my passwords to anyone
- I will be responsible for my behaviour and actions when using technology (Teams meetings, and other interactive applications), this includes the resources I access and the language I use
- I will make sure that all my communication with students, teachers and others using technology is responsible and sensible
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across such material, I will report it immediately to my teacher or parent
- I will not attend live online lessons or assemblies unless I have been invited to do so by a member of staff
- I will not share invitations to online live lessons or assemblies with anyone else
- I will not record or take photos of my classmates or teachers during online home learning
- I understand that when using Google classroom and other applications for school that my use can be monitored and recorded and made available to my teachers for training and safeguarding purposes
- I understand that these rules are to keep me safe and that if they are not followed, school sanctions will be applied in line with the behavior, rewards and sanctions policy and my parent(s) may be contacted.

Guidelines

When participating in online lessons, remember that this is an extension of the classroom and you should conduct yourself as you would in the classroom. This includes:

- Joining in online lessons from an environment that is quiet, safe and free from distractions (preferably not a bedroom)
- Be on time for your online lesson
- Be dressed appropriately for learning (no pyjamas, loungewear, etc)
- Remain attentive during sessions
- Do not have any social media, games or any other applications open on your phone or laptop while participating in a lesson

- Interact patiently and respectfully with your teachers and classmates
- Mute your microphone whenever you aren't speaking in a lesson
- Turn on captions if you are struggling to hear what people are saying
- Provide feedback to teachers about your experiences and any relevant suggestions
- You MUST NOT record each other's online interactions
- Make sure you end the session as soon as your teacher indicates to do so
- If you have any concerns about the behaviour of participants in an online lesson, report them immediately to a parent or the school via dsl@claremont.surrey.sch.uk.