# Online Safety Policy

**School Division:** Whole
**Policy Division:** Safeguarding
**Policy Owner:** Principal
**Date:** September 2025
**Review Date**: September 2026

## Contents

# 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, and visitors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile phones.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

# 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for principals and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

# 3. Roles and responsibilities

## 3.1 The Whole School Leadership Team

The WSLT  has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The DSL will coordinate regular meetings with appropriate staff to discuss online safety,

The governor who oversees online safety is Nickie Moore, Regional Safeguarding Manager for the International School's Partnership.

All governors will:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

## 3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

## 3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular updates on online safety in school to the principal and/or governing board

This list is not intended to be exhaustive.

## 3.4 The Head of IT

The Head of IT is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Communicating any online safety incidents are communicated to the DSL

### 3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by logging them on myconern.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Understanding that systems of Filtering and Monitoring are not 100% effective in keeping children safe. All staff are therefore required to actively monitor students use of technology whilst in their supervision.

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems, and Bring Your Own Device policies.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the ICT curriculum.

Reception - Year 3, Online safety is taught in IT lessons, and PSHE with their form tutor.

Year 4-8 Online safety is taught by the Head of ICT at Claremont Prep, and during PSHE lessons

Year 9-12 Online Safety is taught within PSHE lessons.

The whole school follows Safer Internet day in February.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

**All** schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

# 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, newsletters, or online forums. This policy will also be shared on our website https://www.claremontschool.co.uk/our-school/policies/ .

Online safety will also be covered during parents' evenings.

The school will let parents know what systems the school uses to filter and monitor online use.

We force Google Safe Search on School owned Chromebooks and within the school, we filter all internet traffic via cloud-based filtering (https://www.scoutdns.com/) and block any other traffic using on-site firewalls. We also use Smoothwall Filter and Smoothwall Monitor on all School managed devices.

Smoothwall Monitor is a digital monitoring solution that flags incidents as they happen by real-time monitoring of both keystroke and screen view activity by users.

Safeguarding staff are informed automatically, and in some cases, via a direct phone call, when users try to view or type harmful content. This is installed on all student devices owned and managed by the school.

Smoothwall Filter is an internet content filtering service that is also installed on all student devices owned and managed by the school. This level of filtering will work on and off-site to ensure that the content they are accessing is safe and approved.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the principal.

# 6. Cyber-bullying

## 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

## 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

## 6.3 Examining electronic devices

The Principal, and any member of staff authorised to do so by the principal (Further details can be found in searching and confiscation policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to authorised staff members to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image

- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

# 7. Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3).

For staff this is found within the school's code of conduct

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

We force Google Safe Search on School owned Chromebooks and within the school, we filter all internet traffic via cloud-based filtering (https://www.scoutdns.com/) and block any other traffic using on-site firewalls. We also use Smoothwall Filter and Smoothwall Monitor on all School managed devices.

Smoothwall Monitor is a digital monitoring solution that flags incidents as they happen by real-time monitoring of both keystroke and screen view activity by users.

Safeguarding staff are informed automatically, and in some cases, via a direct phone call, when users try to view or type harmful content. This is installed on all student devices owned and managed by the school.

Smoothwall Filter is an internet content filtering service that is also installed on all student devices owned and managed by the school. This level of filtering will work on and off-site to ensure that the content they are accessing is safe and approved.

Student owned device access to the internet is filtered via cloud based filtering (https://www.scoutdns.com/). Students are only allowed to use their own devices in the presence of a teacher or appropriate adult, to ensure effective monitoring of internet usage,

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

# 8. Students using mobile devices in school

**Prep School**

Students are not permitted to use mobile phones at the Prep School. In extenuating circumstances, parents can ask the principal for permission for their child to bring their mobile device. If a student brings a phone into school, it must be taken at the beginning of the day to the Main Office and kept in the designated storage box. Phones are collected at the end of each school day. If a student brings a phone without permission, this is confiscated and the parent must collect the device. The students will be reminded why phones are not permitted within school.

**Senior School**

Mobile phones are not permitted at the senior school between years 9-11. Any student seen with a mobile phone, will have it confiscated. A parent or carer will need to come into school to collect the mobile phone.

In year 9-11 specific permission may be given for a student to bring a mobile phone into school. The request must be made in writing to the students HOH, eg for reasons such as a complicated journey home. If permission is granted, students must hand their mobile phone into the office, on arrival at school.

Sixth formers are allowed to use mobile phones at school. They are asked to refrain from suing them around the school site, only using them freely in the sixth form building.

## 9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates, and maintaining anti-virus and anti-spyware software

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Andy Clifton (IT manager)

## 10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our IT, Acceptable use and Behaviour policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and Disciplinary procedure policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log will be kept on MyConcerns.  This policy will be reviewed every year by the DSL's. At every review, the policy will be shared with the governing board.

### 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

**Appendix 1**


**All pupils at Claremont School will review the content of this agreement in their IT lessons. The meaning and implications of each section will be discussed.**

## CLAREMONT PREP SCHOOL IT ACCEPTABLE USE AGREEMENT

The following refers to the use of Claremont School's Google Learning Platform and hardware used within school. This Agreement is in addition to the Video Conferencing Agreement (used during Online Learning).

**Link to IT acceptable use agreement form (prep)**

This is how we stay safe when we use computers

I will uphold the school rules and values both online and offline

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use - this includes accessing inappropriate websites
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will treat my username and password with care. I will not share them, nor will I try to use any other person's username and password
- I will not share images of other students or members of the school community eg. teachers without their permission
- Always log off or sign out of a computer when I have finished working
- I will not open attachments or links in emails without first checking with a teacher or responsible adult
- I will tell a teacher or suitable adult if I see something that upsets me on the screen

- I will use my school account appropriately and not use it to access websites, apps, games that are not appropriate for my age
- I will be polite and responsible when I communicate with others, I will not use aggressive or inappropriate language
- I understand that cyberbullying is unacceptable and will not be tolerated at Claremont school. I will not use my school account (or any account) for cyberbullying
- I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me. I understand that for my safety, school staff monitor my use of the school I.C.T. systems, email and other digital communications

I understand that if I fail to comply with this Acceptable Use Agreement, a sanction may be given. This may include Stripe/Negative comment, Detention or Exclusion from Claremont School,

Signed (child):…….. Date:

## Appendix 2

# Claremont Senior School Online Safety and Bring Your Own Device Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure that students, parents, and staff understand the responsibilities associated with the safe, ethical, and lawful use of technology at Claremont School. It applies to all technology resources, including personally-owned and school-provided devices. All users of Claremont School's network or digital technology are expected to act responsibly, respectfully, and in accordance with this policy at all times.

In the event of a breach of this agreement:

- Student technology privileges may be suspended or revoked, and
- Disciplinary action may be taken, in line with Claremont School's Behaviour and ICT policies.

This policy applies to all devices used at Claremont School — whether owned by the school or the student. Additional requirements or guidelines may be set by teachers for use in specific lessons or activities.

**Phone Usage**
Mobile phones are not permitted in school for students up to and including Year 11. If it is necessary for a student to have a mobile phone for their journey to school, permission must be granted by their parent/guardian, and the Use of Mobile Phone form completed.

Students with permission to have a mobile phone for their journey to school must hand in their mobile phone to the school office as soon as they arrive at school.

Any student up to and including Year 11 found with a mobile phone during the school day will have it confiscated, and stored securely at school, to be collected by a parent or guardian at their convenience. Phones are only returned to students directly at the end of the last day of each half term.

Students in Year 12 and 13 are allowed to use mobile phones in the Sixth Form Centre.

**Headphone Usage**
Students up to and including Year 11 are only allowed to use headphones under the direction of a member of school staff (e.g. in a lesson, as part of a listening exercise). Students using headphones outside of a classroom will have them confiscated and will require collection under the same conditions as a mobile phone.

**Online Safety Agreement**

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies, for school purposes.

- I will keep to the school rules when using my own devices.

- I will not download or install software on school ICT equipment without permission.

- I will only log on to the school network/learning platform with my own school username and password.

- I will follow the school's ICT security system and not reveal my passwords to anyone.

- I will only use my school email address to log into Google when accessing digital technology at school.

- I will make sure that all ICT communications with pupils, teachers or others are responsible and sensible.

- I will never post aggressive or offensive material on the system or the internet at any time.

- I will respect the privacy and ownership of others' work online at all times.

- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.

- I will not attempt to bypass the internet filtering system. I will not use a VPN whilst using the school network.

- I will ensure that my online activity, both in school and outside school, will not cause distress or bring the school, staff, or pupils into disrepute.

- I understand that these rules are designed to keep me safe, and that school sanctions will be applied if they are not followed. My parent/guardian may be contacted.

- I will be very careful about giving out personal information such as name, phone number or address online. I will not post my personal information publicly.

- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with school policy. I will not distribute images outside the school network without permission.

-I will not participate in or encourage online bullying or harassment.

- I understand that my use of Claremont's systems is monitored and logged, and may be accessed by teachers.

- If anything makes me uncomfortable or worried, I know that I can speak to a teacher or parent without being blamed.

- I will only use a student owned device when supervised by a teacher, or appropriate adult, in order to ensure appropriate monitoring can take place.

-I will use AI tools ethically, in line with academic honesty and plagiarism guidelines. I understand the school uses software to detect the use of plagiarism for assessment purposes. Plagiarism may result in school disciplinary action, and potentially disqualification from exam board qualifications.

- **I understand that the school has a legal responsibility to filter and monitor online activity. By using a school or student-owned device on the Claremont School network, I understand that the school may monitor usage and has the right to confiscate and, if there is reasonable suspicion of misuse, search the device in accordance with school safeguarding procedures.**

**Agreement & Signature**

I understand and agree to follow the terms of the Claremont School Online Safety and BYOD Acceptable Use Agreement. I am aware that failure to follow these rules may result in disciplinary action, including loss of technology privileges.

Student Name: _____

Student Signature _____

Date _____

**All Staff will be aware of the IT Acceptable Use Agreement.**

| |
|---|
| **When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**<br>● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)<br>● Use them in any way which could harm the school's reputation<br>● Access social networking sites or chat rooms outside required for job role<br>● Use any improper language when communicating online, including in emails or other messaging services<br>● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>● Share my password with others or log in to the school's network using someone else's details<br>● Take photographs of pupils without using a school device<br>● Share confidential information about the school, its pupils or staff, or other members of the community<br>● Access, modify or share data I'm not authorised to access, modify or share<br>● Promote private businesses, unless that business is directly related to the school |
| I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.<br>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.<br>I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. |