CPS Online Safety Policy

Date Written	**September 2024**
Next Review	September 2026
Online Safety Leads	Hilary Ali & Mike Godfrey

Online Safety Policy

Introduction

At Claygate Primary School we respect every child's need for, and rights to, an environment where safety, security, praise, recognition and opportunity for taking responsibility is available. This policy is informed by our vision:

Our vision is to develop high achieving, aspirational, confident and responsible individuals. We will do this by proving a welcoming and happy school community within a safe and supportive learning enrichment, where all achievements are valued and celebrated.

Aims

Claygate Primary School aims to:

• Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
• 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 and smart technology (which we refer to as 'mobile phones')
• Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The School's 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, antisemitism, 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
• ***Commerce*** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2022, and its advice for schools on:

• Teaching online safety in schools
• Preventing and tackling bullying and cyber-bullying: advice for headteachers 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.

The policy also takes into account the National Curriculum computing programmes of study.

Role and Responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation. The Governing Body will co-ordinate half-termly meetings with the Safeguarding Team to discuss online safety, and monitor online safety logs.

The governor who oversees online safety is Rachael De Vizio.

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 (see Appendix)
• Ensure that online safety is a running and interrelated theme while devising and implementing the whole school approach to safeguarding and related policies and/or procedures
• 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.

The Head Teacher

The Head Teacher is responsible for ensuring that all CPS staff understand this policy, and that it is being implemented consistently throughout the School.

The Safeguarding Team

Details of the school's Safeguarding Team are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions. In addition, a poster is displayed throughout the school giving details of the DSL team. The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety in school, alongside our computing lead, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the School
- Ensuring that all staff understand the CPS Acceptable Use Policy and are clear on filtering and monitoring systems used in school
- Working with the Head Teacher and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the School's Child Protection and Safeguarding Policy
- Ensuring that any online safety incidents are logged on CPOMS 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's Behaviour and Anti-Bullying policies
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head Teacher and/or Governing Body

The ICT Technician (Eduthing IT Services for Education)

The ICT Technician 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 (at CPS we use SENSO)
• Ensuring that the School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
• Conducting a full security check and monitoring the School's ICT systems on a fortnightly basis
• Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All Staff and Volunteers

All staff, including contractors and agency staff (where appropriate), and volunteers (where appropriate) 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 (see Appendix), and ensuring that pupils follow the School's terms on acceptable use (see Appendix)

• Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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's 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'

Parents and Carers

Parents and carers are expected to:

• Notify a member of staff or the Head Teacher 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 internet (see appendix)

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 (regular updates from Childnet are provided via the CPS weekly parent newsletter)

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 (see Appendix).

Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum – National Curriculum computing programmes of study. 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

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

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. At CPS we follow the KAPOW scheme of work for Computing which includes content for all year groups on keeping safe online. Online Safety is also taught explicitly through our PSHCEE Curriculum (Jigsaw scheme). In addition, we hold Safer Internet Day each year and hold workshops to further educate children on this topic.

Educating Parents About Online Safety

At CPS we will raise parents' awareness of internet safety via weekly newsletters or other communications home, and in information via the school website. This policy will also be shared with parents on the school website. In addition, we offer an online safety session for parents annually, this is delivered through Childnet.

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

Cyber-Bullying

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. At Claygate primary School we use S.T.O.P. (Several Times On Purpose) to describe bullying. Please also the School's Behaviour and Anti-Bullying policies.

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. 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.

In relation to a specific incident of cyber-bullying, Claygate Primary School will follow the processes set out in our 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. Where appropriate the DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police** *

If a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the Safeguarding Team immediately, who will decide what to do next. The Safeguarding Team 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.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence. 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

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the School's Complaints Policy.

Acceptable Use of the Internet in School

All pupils, parents, staff, and governors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet (see Appendices).

Visitors and volunteers will be expected to read and agree to the school's terms on acceptable use if relevant. These terms are stated in the safeguarding leaflet given to all visitors on entry to the school site.

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, governors, visitors and volunteers (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in the appendices to this policy.

Pupils Using Mobile Devices in School

Mobile phones – Pupils in year 6 (and some in Year 5 with prior agreement from the school) may bring mobile phones into school, but are not permitted to use them during the school day. They should be handed in to their class teacher and they will be stored in a locked cupboard for the day. Mobile phones must be switched off once pupils have crossed the threshold of the school gates in the morning.

Parents and Pupils agree to ensure that there are no apps on phones bought into school that are targeted at age 13+. This is made explicit to parents via a consent for mobile phone document which must be signed prior to permission being given.

Smart Watch – At Claygate Primary School we encourage children to wear watches in school, although we do not allow 'smart' watches to be worn, or any watch that has the same functionality as a mobile phone or PC, on the school site.

Laptops/ tablets – If the parents/carers have agreed with the SEND team that their child should use a laptop or tablet in school this must be set up on the schools network therefore ensuring it has the appropriate level of security protection. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendices).

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 using strong passwords
• Only use USB sticks if they are encrypted – this means if the device is lost or stolen, no one can access the files stored on it
• When working on school documents access and save them via the server remotely using remote desktop access
• Making sure the device locks if left inactive for a period of time
• Not sharing the device among family or friends
• Installing anti-virus and anti-spyware software
• Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the Appendices. Work devices must be used predominantly for work activities. If staff have any concerns over the security of their device they must seek advice from our ICT technician, Eduthing IT Services for Education.

How The School Will Respond To Issues of Misuse

Most issues of misuse will take place outside school. It is the School's responsibility to educate the children to try and reduce the number of incidents and encourage the children to both talk about anything that has happened and to recognise the dangerous/challenging situations that they may find themselves in.

We strongly encourage parents and carers to monitor their children's online activity on all devices thus helping reduce the numbers of incidents and to communicate with the School if any incidences occur as soon as they become aware.

Where a pupil misuses the School's ICT systems or internet in school, we will follow the procedures set out in our Behaviour and Anti-Bullying policies. 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. 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.

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, online newsletters and weekly staff briefings).

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
• the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
• the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our Child Protection and Safeguarding Policy

Monitoring Arrangements

Safeguarding issues related to online safety are logged on CPOMS and a termly analysis is completed and shared with the Governing Body at FGB meetings.

This policy will be reviewed every year by the Deputy Designated Safeguarding Lead and, at every review, will be shared with the Governing Body.

Links With Other Policies

This Online Safety Policy is linked to our:
Child Protection and Safeguarding Policy
Behaviour Policy
Anti-Bullying Policy
Staff Code of Conduct
Data Protection Policy and
Privacy Notices
Complaints Policy