THE CAMBRIDGE PRIMARY SCHOOL

Online Safety & Smartphone Policy

Date of Approval:	March 2026
Date of Next Review:	March 2027

The Cambridge Primary School
Queens Avenue, Wellesley
Aldershot, Hampshire GU11 4AA
01252 314884

Online Policy & Smartphone Policy

Introduction

This policy sets out how The Cambridge Primary School safeguards pupils and staff in relation to online activity, digital technology and the use of smartphones and other internet-enabled devices. It should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Acceptable Use Agreements and relevant data protection procedures.

Purpose

The purpose of this policy is to:

- Safeguard and protect all members of The Cambridge Primary School's community in their use of digital technology.
- Set out the school's expectations for safe, responsible and respectful online behaviour.
- Identify approaches to educate and raise awareness of online safety and digital well-being throughout the school community.
- Enable all staff and children to work safely and responsibly, model positive behaviour online, and manage personal data and information effectively.
- Establish clear mechanisms to identify, intervene, and escalate any incident where appropriate.
- Identify the risks associated with smartphone use and establish guidelines for their use within the school environment.
- Promote awareness among pupils, staff, and families about responsible internet use.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers, and governors.
- Identify and support groups of children that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety that empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (referred to as 'mobile phones').
- Establish clear mechanisms to identify, intervene, and escalate an incident where appropriate.

Key Categories of Risk

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

1. **Content:** Exposure to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
2. **Contact:** Being subjected to harmful online interaction with other users, including peer pressure, commercial advertising, and adults posing as children or young adults with the intent to groom or exploit.
3. **Conduct:** Online behaviour that increases the likelihood of, or causes, harm, such as the making, sending, and receiving of explicit images (both consensual and non-consensual), online bullying, and other harmful behaviours.
4. **Commerce:** Risks associated with online gambling, inappropriate advertising, phishing, and financial scams.

This policy applies to all members of The Cambridge Primary School community (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

Roles and Responsibilities

Role	**Person(s) Responsible**
Designated Online Safety Lead	Josh McCormack (DDSL)
Designated Safeguarding Lead (DSL)	Sue Tancock (HoS)
Monitoring Digital Activity on School Systems	Sue Tancock (HoS)
Filtering and Monitoring Systems effectiveness	Josh McCormack (DDSL) & Sue Tancock (HOS)
Governor Representative (Filter and Monitoring)	Melanie Barrie (VCoG)
Governor Representative (Safeguarding)	Theresa Pitfield (CoG)

Local Advisory Committee (LAC) (Governing Body)
The LAC should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Headteacher and Senior Leadership Team
The headteacher and senior leadership team are responsible for ensuring:

- The Online Safety & Smartphone Policy is implemented and compliance with the policy is monitored.
- Staff receive suitable training and development to carry out their online safety roles.
- Robust reporting channels for online safety concerns and incidents exist (the school currently uses SENSO, CPOMS and CEOP reporting tool)
- Online safety issues are embedded in all relevant school policies and procedures.
- Appropriate and effective filtering and monitoring systems are in place for pupils when using school devices.

Designated Online Safeguarding Lead – Mr McCormack
The DOSL is responsible for:

- Leading day-to-day online safety issues and reviewing the school's online safety policies and procedures.
- Ensuring online safety is recognised across all safeguarding and child protection work.
- Coordinating participation in local and national online safety initiatives – including keeping up-to-date training from NCA (National Crime Agency) with CEOP Ambassador, annual training.
- Ensuring that online safety training for staff is integrated, current, and relevant.

All Staff
All staff have a duty of care to ensure the safety of children and to report any concerns about online safety to the DOSL or a member of the DSL team.
Staff are responsible for:

- Consistently enforcing this policy within the school.
- Modelling positive online behaviours and promoting a culture of online safety and smartphone usage.
- Embedding online safety in their teaching and school activities.
- Monitoring children's online activity and reporting any concerns.

- Maintaining an awareness of current online safety issues and guidance.
- Minimise their use of mobile phones for personal reasons to model appropriate behaviour.
- Only using school provided email accounts to access pupil data and using two-factor authentication.

Children

Children are responsible for:

- Engaging in age-appropriate online safety education.
- Knowing and adhering to school rules and policies regarding the use of digital technologies.
- Respecting the feelings and rights of others both online and offline.
- Seeking help from trusted adults if they are concerned about something they have seen or experienced online.
- Only using school provided email accounts for educational purposes.

Parents and Carers

Parents and carers have an essential role in ensuring their children use digital technologies safely and responsibly both in and out of school. Parents and carers are responsible for:

- Modelling positive online behaviours and promoting a culture of online safety and smartphone use at home.
- Discussing online safety with their children and reinforcing the school's approach and expectations.
- Keeping up to date with online safety issues and the school's Online Safety Policy.
- Informing the school of any online safety concerns that may impact their child or other children at the school.

Acceptable Use

All members of the school community must adhere to the following acceptable use guidelines:

- Use school devices for educational purposes only
- Personal devices connected to the school network (for example governors requiring access for meetings) must be used in accordance with this policy
    - Any person wanting to connect a device to our network needs to declare the device's ID.
- Do not access, share, or create inappropriate content or engage in any form of online bullying.
- Report any online safety concerns to a trusted adult immediately.

Use of Work Devices Out of School

- School-owned devices may only be used outside of school for educational purposes as directed by The Senior Leadership Team.
- Staff must ensure that sensitive information is stored securely, and devices are returned to school in good condition.
- Children must not take school devices home without prior permission and must adhere to the school's acceptable use policy at all times.

Smartphone-Free School for Pupils

The term smartphones also includes smart enabled devices, such as, but not limited too smart watches or anything that can communicate to the internet.

The Cambridge Primary School operates a smartphone-free environment for pupils. Pupils must not bring smartphones, smartwatches or other internet-enabled personal devices onto the school site, on educational visits or on residential visits unless an exception has been formally agreed by the Headteacher.

Where a phone is needed for travel arrangements, only a basic mobile phone (Brick or chocolate bar type) that allows calls and texts but has no internet access, camera or app capability may be permitted for pupils in Years 5 and 6. Any such device must be handed to the class teacher on arrival and collected at the end of the school day.

Exceptions will only be agreed in exceptional circumstances, including medical, safeguarding or additional needs, and will be recorded and reviewed on an individual basis.

The Cambridge Primary School does not support primary-aged children owning or routinely using a smartphone. In line with current Department for Education (DfE) guidance, the school promotes a mobile phone-free environment for pupils because:

- Development of critical thinking and emotional regulation skills.
- To reduce distraction and disruption, support learning and behaviour
- Encouragement of real-life social interactions.
- Reduction of privacy risks and online dangers.

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences. There will also be opportunities for parents to engage with workshops and appropriate guidance regarding keeping children safe online.
- The Cambridge Primary School promotes a smartphone-free environment to encourage face-to-face interaction and reduce distractions **(this is during the time any child is on the school premises, school trips and residentials).**
- Children are not permitted to have smartphones on school premises unless prior arrangements have been made with the Headteacher under medical grounds.
- Parents are encouraged to support this policy by ensuring that children do not bring smartphones to school.
- In the event of a child having a smart phone in school, it will be reported to the DOSL and reasonable steps will be made to address concerns and risks.

Risks Associated with Smartphone Use

Smartphones offer advanced features, including internet access and social media, which can lead to various risks:

- Cyberbullying: Smartphones can facilitate harassment, making it difficult for pupils to escape bullying.
- Exposure to inappropriate content: Unfiltered internet access can expose children to unsuitable material.
- Mental Health Concerns: Excessive use can contribute to anxiety and depression.
- Distraction from Learning: Smartphones can disrupt the learning process.
- Privacy and Security Risks: Children may not understand how to protect their personal information, leading to exploitation.
- Self-obsession and Personal Curation: The culture of selfies and social media can create confidence issues.

Cyber Bullying

Cyber Bulling is defined as any targeted use of digital technology (such as text messages, social media, or messaging apps) to intimidate, threaten, or harm another person.

This can be a complex area, and these examples might help:

- A child is receiving taunts on social media and text from an ex-pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.
- A child is receiving taunts from peers. It is all at weekends. The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.
- A child is receiving taunts from peers. It is all at weekends using social media. The pupils are in Y5: The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of social media outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school, the school could legitimately say that the victims and perpetrators had failed to follow the school's recommendation. They could then deal with residual bullying in the school but refuse to deal with the social networking issues.
- Once disclosure is made, investigation will have to involve the families. This should be dealt with under the schools anti-bullying policy and child-on-child guidance within the safeguarding and child protection policy.
- If parents or carers fail to engage and bullying continues, the school may refer the matter to the police under relevant legislation, including offences related to harassment or malicious communication.

Confiscation and Sanctions

- The school reserves the right to use sanctions for breaches of the mobile phone policy, including confiscation and suspension.
- The final decision on what constitutes a smart device lies with the -DOSL and the Head Teacher.
- Any smartphone or internet-linked device found on school premises will be confiscated and returned only to a parent or carer.
- 'Brick' phones are permitted for the journey to and from school for Years 5 & 6, but if they are not handed in to the class teacher during school hours, they will also be confiscated and returned to a parent or carer.
- Repeated violations may result in consequences in line with our Behaviour Policy.
- In line with legislation, staff are protected from liability when confiscating items if they act lawfully and proportionately.

Encouragement of Alternatives

- If parents wish to consider alternatives such as electronic tags or trackers for location monitoring instead of smartphones, they are welcome to do so, however these will not be allowed on residentials or school trips.
- Alternative phone options which allow for location monitoring and GPS.
- Where children are due to attend school trips or off site visits we do not allow the use of any tracking or GPS device for an individual child. This causes increased risk to all children involved and is against our safeguarding and child policy.

Critical Incident Management

In the event of an online safety incident, the school will:

- Follow established procedures for reporting, recording, and responding to incidents.
- Ensure that all staff are trained to manage online safety incidents effectively.
- Provide support and guidance for those affected by online safety incidents.

- Review and adapt policies and procedures following any critical incident to improve future responses.

Monitoring and Review
The Cambridge Primary School will regularly monitor and evaluate the implementation and effectiveness of this Online Safety & Smartphone Policy, including:

- Annual review of the policy and associated procedures.
- Monitoring of online safety incidents and concerns.
- Gathering feedback from the school community on the policy and its implementation.
- Keeping up-to-date with the latest online safety guidance and best practises.

Communicating the Policy

- The policy will be communicated to all members of the school community, including pupils and parents, to ensure clarity and consistency in its implementation.
- Regular reminders will be provided to pupils about the policy and its rationale.

Reporting Concerns
If any pupil, staff member, or family has concerns regarding internet or mobile phone use, they should report it to the school's Designated Safeguarding Lead, who will liaise with the Designated Online Safeguarding Lead. All concerns will be treated seriously and addressed in line with the school's safeguarding and behavioural policies.

Conclusion
The Cambridge Primary School is committed to ensuring the online safety of all members of its community. This policy, along with our safeguarding policy, provides a comprehensive framework to guide the school's approach, ensuring that all stakeholders understand their roles and responsibilities in maintaining a safe online environment. It also addresses the potential dangers of smartphones while promoting responsible habits among pupils. We invite parents to collaborate with us in creating a culture of safety and respect within our school community.

At The Cambridge Primary School, we are dedicated to creating a safe and nurturing environment for all our pupils. Recognising that mobile phones have become ever-present among children, we understand the need for a comprehensive online safety and mobile phone policy that addresses the potential dangers associated with their use. This policy aligns with our safeguarding policy and emphasises our commitment to pupil well-being.

Together, we can help protect our pupils from the dangers of smartphones and guide them toward healthier technology use.

Designated Online Safeguarding Lead: Mr Josh McCormack
In the absence of the above named person, DSLs will take responsibility.

Appendix 1: Online Safety and Internet Use Agreement for Parents and Pupils

Parents are encouraged to:

Parents and carers are expected to support the school's online safety approach by actively discussing online risks with their children and reinforcing safe, responsible behaviour at home.

They should also model appropriate use of technology and social media by:

- Staying informed about online safety guidance through school communications, the website, online safety workshops, or personal research.

- Ensuring their child uses only age-appropriate apps and games and is not exposed to unsuitable content.
- Respecting age restrictions on social media platforms and understanding the potential risks of early access.
- Avoiding any online content that could lead to legal or reputational harm – including material that is illegal, offensive, defamatory, or discriminatory.
- Ensuring that social networking apps (including WhatsApp) are never used in an abusive or hateful manner.
    - **Not discussing the school or staff on any WhatsApp groups, and ensure any concerns are brought to the school first.**
- Not sharing photos or videos of school events (e.g. Christmas productions) on social media if they include children other than their own, unless consent has been obtained from both the child and their parent.
- Only taking photos at school events with the Headteacher's permission – and using them strictly for personal use (not online sharing).
- Talking to their child about consent and the importance of respecting others when sharing images online, even of their own child (also known as "sharenting").
- Avoiding any online references to staff, pupils, or other parents without explicit consent.
- Support the school's ban on smartwatches and smartphones in line with safeguarding expectations, ensuring their child does not bring internet-connected devices to school unless agreed with the Headteacher/ DOSL.

Pupils are encouraged to:

- Build computing and research skills through safe use of technology.
- Take part in online learning, including age-appropriate games and quizzes.
- Learn and apply the SMART Rules to stay safe online.
- Report any inappropriate contact or cyberbullying to a trusted adult immediately – the school has a zero-tolerance policy for cyberbullying.

Pupils are not permitted to:

- Download software or files without permission from a teacher or parent.
- Send or take part in inappropriate, abusive, or harmful messages or online chats.
- Share personal information about themselves or others (e.g. addresses, phone numbers, photos).
- Use someone else's login or share their own passwords.
- Access social networking sites during the school day.
- Attempt to connect with staff on social media — any attempt will be reported to the Headteacher and parents informed.
- **Bring smartphones or smartwatches to school**, unless agreed with the Headteacher for medical reasons

Sanctions:

- Verbal warnings – These are given for attempts to contravene the rules.
- A written letter to parents stating what has occurred. The pupil's Internet use at school will then be monitored for a reasonable period.
- In some cases, the child will lose access rights to the school Internet for an appropriate period of time. This decision will be made by the Leadership Team/ DOSL.

Appendix 2: Pupil Online Safety Agreement (Reception)

These rules will help to keep everyone safe and help us to be fair to others.

- I will only go on apps that adults have told me to go on.
- I will only visit Internet sites that are appropriate for my age.
- I will only talk online with people I have met and know.
- I will only send kind messages.
- I will not open anything unless I have been given permission by an adult.
- I will not post anything online without telling an adult.
- If I see anything I do not like, I will show an adult.

My name: . . . . . My class: . . . . . .

Parent Online Safety Agreement

As the parent or legal guardian, I have read and understood the school's online safety rules and give permission for my child to use the internet and school computing facilities.

We have discussed the rules together, and my child understands the importance of using technology safely and responsibly at The Cambridge Primary School.

I understand the school takes reasonable precautions to protect pupils online, including filtered internet access, monitoring systems, and online safety education. While the school cannot be held responsible for all internet content, I acknowledge their commitment to keeping children safe.

I am aware that the school may monitor my child's files and internet activity, and will contact me if concerns arise about their online behaviour or safety.

I accept that the school is not liable for any damage caused by my child's use of internet services.

I support the school's **smartphone-free policy**, which does not allow children to bring smartphones or smartwatches to school unless agreed with the Headteacher on medical grounds. I will ensure my child follows this policy.

I will also promote safe use of the internet and digital technology at home, and share any concerns about my child's online activity with the school.

Child's name: …….. Child's class: ……..

Parent/Guardian signature: …….. Date **……**

Appendix 3: Pupil Online Safety Agreement (KS1 and KS2)

These rules will help keep everyone safe and fair online:

The Cambridge Primary School
Queens Avenue, Wellesley
Aldershot, Hampshire GU11 4AA
01252 314884

- I will only use the school's computers for schoolwork and homework. When in a club, I will make sure to use them appropriately and go on the programs that the adults have told me to.
- I will only edit or delete my own files once I have asked an adult.
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them.
- I will only talk to people I know or that a trusted adult has approved.
- I will send only kind and polite messages.
- I will not open an attachment, or download a file, unless I have been given permission by an adult.
- I will not share personal information (like my name, address, phone number or photos) unless a trusted adult says it's okay.
- I will ask an adult before editing or deleting any of my files.
- I will tell a trusted adult if I see something online that makes me feel worried, upset or unsafe.
- I will not bring a smartphone or smartwatch to school unless my parent or carer has agreed this with the Headteacher.

My name: . . . . . My class: . . . . . .

Appendix 5: Filtering and Monitoring at The Cambridge Primary School

Learn about our school's filtering and monitoring systems and how you can help to keep pupils safe online and know what to do if you have concerns about the content that pupils are accessing.

What is filtering and monitoring?

Filtering systems block access to harmful websites and content.

Monitoring systems:

- Identify when someone searches for or tries to access certain types of harmful online content on school devices
- Identify who is searching for or accessing the harmful content
- Alert the school about it so we can intervene and respond
- **Don't** block access to harmful content

We're all responsible for filtering and monitoring

No filtering and monitoring software is perfect:

- It might not be aware of all the websites that contain inappropriate content
- Abbreviations or misspellings in a search engine may slip past the software
- Inappropriate content may be found on websites considered 'safe'

You can help to make sure the internet is used appropriately by:

- **Monitoring** what pupils are accessing on devices during school hours (e.g. by looking at their screens when using computers during lessons).
- **Teach** children about responsible digital behaviour, ethics, and the consequences of inappropriate online actions.

- **Alerting** Sue Tancock or another member of the DSLTeam, if you become aware that content is not being filtered or if you have concerns about what a pupil is accessing online.

Inappropriate content includes:

- Illegal content (e.g. child sexual abuse)
- Discriminatory content (e.g. sexist, racist or homophobic content)
- Sites that promote drugs or substance abuse
- Extremist content (e.g. the promotion of terrorism)
- Gambling sites
- Malware and/or hacking software
- Pornography
- Pirated material (copyright theft)
- Sites that promote self-harm, suicide and/or eating disorders
- Violent material

What systems do we use?

Keeping Children Safe in Education 2024 states that all schools should have appropriate filtering and monitoring systems in place.

We have the following systems in place:

Filtering: LGFL

What is it? Content control – blocking or allowing content using URLs, keywords, content categories.

What does it do? **Protects** from harm (but no guarantees, not 100%), **minimises distractions** from learning, **needs to be balanced** – protection v over-blocking, tends to be **reactive**.

Monitoring: SENSO and staff

What is it? Supervision (physically or via tech) of what children and staff are accessing.

What does it do? Protect from online bullying, **verify** learners are acting responsibly and learning acceptable online behaviour, **ensure** the filtering **system is working** well, and **provide** a **safe** place to learn from mistakes.

Our School Response to Filtering and Monitoring Alerts.

- Children use their individual their username and password (Google account) when accessing school devices. This enables any alerts to identify them my name. For laptop and Chromebook access, they must sign in to the school network.
  For iPads, Safari has been disabled and children and staff access the internet through the SENSO APP. They sign in using a generic username and password (different for children and adults). Children must complete the iPad ID monitoring sheet when taking an iPad to use.
- Children must be reminded to sign out of their Google account.
- If attempts to access blocked content with *critical* severity are made:
  - SENSO issues an alert which goes directly via email to the SENSO team (SLT)

- Alerts are acted on immediately, with the 'duty' SENSO team member following up with the child or sending an e-mail to the child's class teacher to follow up later.
  - The status of the alert is edited on SENSO Cloud and explanatory notes added (if necessary).
  - If the alert is triggered by a tracked child or is of a racist, sexual or extremely graphic nature then it will be logged on CPOMS for further follow up.
- If attempts to access blocked content with *low, medium, high* or *urgent* severity are made:
  - They appear on SENSO and are managed by the 'duty' SENSO team member.
  - The status of the alert is edited on SENSO Cloud and explanatory notes added (if necessary).
  - If the alert is triggered by a tracked child or is of a racist, sexual or extremely graphic nature then it will be logged on CPOMS for further follow up.
- A weekly report is run by Sue Tancock (HOS) every Friday and logged in the Safeguarding SharePoint folder.
- The reports are viewed in the weekly DSL meeting every Monday to look for patterns and trends, and identify whether any further action needs to be taken or whether any further words/websites etc may need to be blocked.
- Colin Carpenter & Josh McCormack (DOSL) are responsible for maintenance and review of the software.
- The DSL team are responsible for testing the filtering and monitoring system during the safeguarding meeting on a weekly basis.
- Theresa Pitfield (Safeguarding Governor) & Melanie Barrie (Vice Chair of Governors) are responsible for testing the filtering system on a termly basis.
- Melanie Barrie (Vice Chair of Governors) is responsible for monitoring the level of filtering and monitoring the school undertakes in line with KCSIE

How to raise questions or concerns

Our filtering and monitoring system is designed to protect pupils online. It shouldn't have an impact on teaching and learning or school administration.

Please complete the following form: Internet Filtering Request – Fill in form If you and/or pupils:

- Cannot access content that you need to carry out your work
- Have access to content that should be blocked
- If you become aware of pupils accessing concerning content at any time, report this to Josh McCormack (DOSL) as soon as possible, or please speak to any member of the DSL Team.

Standard	The importance of meeting the standard	How to meet the standard	How CPS meet the standard
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems	Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.	Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. To do this, they should identify and assign: • a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met • the roles and responsibilities of staff and third parties, for example, external service providers We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible and it must be possible to make prompt changes to your provision.	• Theresa Pitfield (Safeguarding Governor) • Sue Tancock (DSL/SLT) is responsible for ensuring that we meet the standards as set out by the DFE. • Colin Carpenter (IT Technician) is responsible for the maintenance of the filtering and monitoring systems.
You should review your filtering and monitoring provision at least annually	For filtering and monitoring to be effective it should meet the needs of your pupils and staff, and reflect your specific use of technology while minimising potential harms. To understand and evaluate the changing needs and potential risks of your school or college, you should review your filtering and monitoring provision, at least annually. Additional checks to filtering and monitoring need to be informed by the review process so that governing bodies and proprietors have assurance that	Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually. The review should be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.	• Weekly Reports run and reviewed in DSL meetings. These enable us to search for patterns and trends, and identify whether any further action needs to be taken or whether any further words/websites etc may need to be blocked. • Filtering and monitoring checked weekly. • Termly Governor checks during Safeguarding meeting. • Provision is reviewed and updated annually using and online safety audit, to ensure it is both effective and meets both the Filtering and Monitoring standards and our needs as a school. onlinesafetyaudit.lgfl.net

	systems are working effectively and meeting safeguarding obligations.	Your IT service provider may be a staff technician or an external service provider.	
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning.	An active and well managed filtering system is an important part of providing a safe environment for pupils to learn. No filtering system can be 100% effective. You need to understand the coverage of your filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty. An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not: • unreasonably impact teaching and learning or school administration • restrict students from learning how to assess and manage risk themselves	Governing bodies and proprietors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college. Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. You may need to ask your filtering provider for system specific training and support.	• LGFL provide our filtering systems. • Weekly tests are run on our filtering system every Monday by the Safeguarding Team as part of the agenda. • Termly tests are run on the filtering system by Theresa Pitfield as part of the termly Safeguarding Governor meeting. • Weekly filtering reports are run every Friday by Sue Tancock and logged in the following location - S:\Safeguarding\Filtering & Monitoring\Filtering Reports\2023-24 • Sue Tancock has received training and attended webinars by LGFL on the topic of Filtering and Monitoring. Advised by IT technician Colin Carpenter and Lisa Crouch. • To ensure that the filtering system does not impact learning, the IT technician can allow access to websites for lessons. This website will be reviewed beforehand to ensure it is appropriate for our pupils. • Our filtering system works in such a way that it does not over block. The focus is the education of pupils.
You should have effective monitoring strategies that meet the safeguarding needs of your school or college.	Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.	Governing bodies and proprietors should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college. The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring. The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective.	• SENSO is the monitoring software that is used within The Cambridge Primary School. • When accessing any school device, all children must be signed in using their Google account individual usernames and passwords to enable any alerts to identify them my name. • For iPads, Safari has been disabled and children and staff access the internet through the SENSO APP. They sign in using a generic username and password (different for children and adults). Children must complete the iPad ID monitoring sheet when taking an iPad to use.

	Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include: • physically monitoring by staff watching screens of users • live supervision by staff on a console with device management software • network monitoring using log files of internet traffic and web access • individual device monitoring through software or third-party services	Training should be provided to make sure their knowledge is current. You may need to ask your monitoring system provider for system specific training and support.	• If attempts to access blocked content with *critical* severity are made: ➢ SENSO issues an alert which goes directly via email to the SENSO team (SLT and Phase Leads) who monitor the email on allotted days. ➢ Alerts are acted on immediately, with the 'duty' SENSO team member following up with the child or sending an e-mail to the child's class teacher to follow up later. ➢ The status of the alert is edited on SENSO Cloud and explanatory notes added (if necessary). ➢ If the alert is triggered by a tracked child or is of a racist, sexual or extremely graphic nature then it will be logged on CPOMS for further follow up. • If attempts to access blocked content with *low, medium, high* or *urgent* severity are made: ➢ They appear on SENSO and are managed by the 'duty' SENSO team member. ➢ The status of the alert is edited on SENSO Cloud and explanatory notes added (if necessary). ➢ If the alert is triggered by a tracked child or is of a racist, sexual or extremely graphic nature then it will be logged on CPOMS for further follow up. • Weekly monitoring reports are run every Friday by Sue Tancock and logged in the following location - S:\Safeguarding\Filtering & Monitoring\Monitoring Reports\2023-24 • The reports are viewed in weekly DSL meeting to look for patterns and trends, and identify whether any further action needs to be taken.

The Cambridge Primary School
Queens Avenue, Wellesley
Aldershot, Hampshire GU11 4AA
01252 314884