THE CAMBRIDGE PRIMARY SCHOOL

ONLINE SAFETY POLICY

2024

Date of Approval:	April 2024
Date of Next Review:	April 2025

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

Contents

Online Safety Policy

Role	Person(s) Responsible	Responsibility
Online Safety Lead	Angela Beeson	Section 1.2.2
Designated Safeguarding Lead (DSL)	Sue Tancock	Section 1.2.2
Governor Representative (Safeguarding)	Theresa Pitfield	Section 1.2.1

The Cambridge Primary School Safeguarding Statement:

At Cambridge Primary School, the Health and Safety of all children is of paramount importance. Parents send their children to school each day with the expectation that our school provides a secure environment in which their children can flourish. We therefore have to ensure that this expectation becomes reality.

Safeguarding determines the actions that we take to keep children safe and protect them from harm in all aspects of their school life. The Cambridge Primary School recognises our moral and statutory responsibility to safeguard and promote the welfare of all pupils. We endeavour to provide a safe and welcoming environment where children are respected and valued. We are alert to the signs of abuse and neglect and follow our procedures to ensure that children receive effective support, protection and justice. Child protection forms part of the school's safeguarding responsibilities and we maintain an attitude of "it could happen here" where safeguarding is concerned.

1. Creating an Online Safety Ethos

1.1 Aims and Policy Scope

- The Cambridge Primary School believes that online safety (sometimes referred to as e-Safety) when using technology such as computers, tablets, mobile phones or games consoles is an essential element of safeguarding children and adults in the digital world.
- The Cambridge Primary School identifies that the Internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- The Cambridge Primary School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- The Cambridge Primary School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.
- The purpose of The Cambridge Primary School's online safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology and to ensure that The Cambridge Primary School is a safe and secure environment.
    - Safeguard and protect all members of The Cambridge Primary School community online with our approach addressing the 4 key 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; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

- Raise awareness with all members of The Cambridge Primary School community regarding the potential risks, as well as the benefits of technology.
- Understand that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. Vulnerable pupils may need adapted online safety education, access and support with support from specialist staff as appropriate, including the Inclusion leader and DSL.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the LAC (Local Advisory Committee), teachers, support staff and visitors who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the Internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as ~~a~~ work laptop, tablets or mobile phones.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding, Anti-Bullying, Behaviour, Data Protection, Online Safety and Internet Use Agreement for Pupils and Parents (See Appendix 1) and Staff Behaviour (code of conduct) policy (including the Acceptable Use Policy).

1.2 Key responsibilities for the community

1.2.1 The key responsibilities of the school management and leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.

- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including the Staff behaviour (code of conduct) policy (including the Acceptable Use Policy) which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems, which meet the needs of the school community, are in place to protect children from inappropriate content whilst ensuring children have access to required educational material (Appendix 5 and 6).
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety, to understand the associated risks and to practise safe online behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the LAC is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

1.2.2 The key responsibilities of the DSL and Online Safety Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.

- Monitor the school's online safety incidents to identify gaps/trends and use this data to update the curriculum accordingly to ensure the school's response addresses this.
- To report online safety concerns and local data/figures, to the school management team, LAC and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school leadership and management to review and update the Online Safety policy, Staff behaviour (code of conduct) policy, Acceptable Use policy and other related policies regularly, with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Ensuring staff are appropriately trained in keeping children safe online, and to undertake training as necessary within this.

1.2.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school's Acceptable Use Policy (AUP), and adhering to it.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site. This includes appropriate use of AI technology.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

1.2.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring learning opportunities are still maximised. Taking responsibility for the implementation of safe security systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.

- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.2.5 The key responsibilities of children and young people, at a level that is appropriate to their individual age, ability and vulnerabilities, are:

- Contributing to the development of online safety policies.
- Reading and adhering to the school Online Safety and Internet Use Agreement for Parents and Pupils (See Appendix 1)
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.2.6 The key responsibilities of parents and carers are:

- Reading the school Online Safety and Internet Use Agreement for Parents and Pupils (See Appendix 1), encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, and other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school's online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

- The school ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information is not published.
- The Headteacher takes overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website complies with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Pupils work may be published with their permission and that of their parents/carers.
- The administrator account for the school website is safeguarded with an appropriately strong password.
- The school posts information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

- Permission from parents or carers is obtained before images/videos of pupils are electronically published – this is provided at point of admission and the confirmed annually. Pupils' consent is also sought.
- The school ensures that all images and videos shared online are used in accordance with parental permission.
- The school ensures that all use of images and videos take place in accordance with other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct and use of personal devices and mobile phones etc.

2.3 Managing email

- Pupils may only use school provided email accounts for educational purposes or where email accounts are necessary to gain access (e.g using an email account to login to a specific software or website).
- In instances where pupils need such accounts, these are provided by the school and, where possible, have email sending and receiving functionality disabled.
- All members of staff are provided with a specific school email address to use for any official communication. These emails are not private and they can be monitored.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.

- Access to school/setting email systems will always take place in accordance with data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff are encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details are not to be used for setting up personal social media accounts.

2.4 Appropriate and safe classroom use of the Internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The school's Internet access is designed to enhance and extend education.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability. The use of learn pads allows teachers to restrict the learners Internet access.
- All school owned devices will be used in accordance with the school Staff Behaviour (code of conduct) policy (including the Acceptable Use Policy) and with appropriate safety and security measure in place. All devices with Internet connectivity functionality will be connected to our secure WiFi which operates a network level filtering and proxy.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet to research, including the skills and knowledge how to locate, retrieve and evaluate information.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The school will use the Internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3. Social Networking and Media

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. Responsible use of social media can be positive for learning and teaching. It can also be personally enjoyable and beneficial.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This guidance is to protect staff, stakeholders and children, in addition to providing a framework of good practice and advising school leadership on how to deal with potential inappropriate use of social networking sites. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The aim of this guidance is to:

- Safeguard children and young people from the potential harm from inappropriate use of social media and networks
- Advise and protect staff from accusations of improper relationships with pupils
- Ensure that the school is not exposed to legal risks
- Ensure that the reputation of the school is not adversely affected
- Ensure that our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school

Social networking applications include, but are not limited to:

- Blogs, for example Blogger
- 'X'
- Online discussion forums, such as mumsnet.com
- Collaborative spaces, such as Facebook
- Media sharing services, for example YouTube

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

When using social media on behalf of the school, staff must be given explicit permission and guidance to use social media on behalf of the school by Headteacher.

- Staff must follow all related procedures when acting on behalf of the school.
- Staff must not use school social media for any personal discussions or for any individual personal matters even if initiated by other members of the school community. Users must be directed to more appropriate communication channels.

3.1 Use of Social Networking sites in work time

Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Headteacher.

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Headteacher first.

Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Headteacher. However, school representatives must still operate in line with the requirements set out within the policy.

School representatives must adhere to the following Terms of Use, this includes for 'Professional Social Networking Accounts'. The Terms of Use below apply to all uses of social networking applications by all school representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. The Cambridge Primary School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

3.2 Terms of Use of Social Networking Applications

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with
- No staff member should have or accept a request from a parent or guardian of a pupil or former pupil on a social networking application
- Where family and friends have pupils in school and there are legitimate family links, please inform the Headteacher in writing. This applies specifically to children
- Employees should not identify themselves as a representative of the school without permission from the Headteacher
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Headteacher

- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action
- It is illegal for an adult to network, giving their age and status as a child
- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the DSL or one of the DDSLs.
- No pupil may access social networking sites during the school day
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Headteacher. Parents will be informed if this happens
- No school computers are to be used to access social networking sites at any time of day.
- Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision
- Pupils should report any improper contact or cyber bullying to their class teacher or another trusted adult in confidence as soon as it happens
- We have a zero tolerance to cyber bullying

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

3.3 Child Protection Guidance

If the Headteacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above they should:

- Record the disclosure in line with their child protection policy.
- Schools must refer the matter to the LADO (Local Authority Designated Officer) and there may be an investigation.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes.
- If disclosure comes from a member of staff, try to maintain confidentiality.
- The Trust will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.
- If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out.

3.4 Cyber Bullying

By adopting the recommended no use of social networking sites on school premises, The Cambridge Primary School protects themselves from accusations of complicity in any cyber bullying through the provision of access.

Parents should be clearly aware of the school's policy of access to social networking sites. Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

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

- A child is receiving taunts on Facebook 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 Facebook. 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 Facebook 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 schools 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 adopted anti-bullying policy and child-on-child guidance within the safeguarding and child protection policy.
- If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment.
- This guidance can also apply to text and mobile phone cyber bullying

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of The Cambridge Primary School community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is defined below.
- The Cambridge Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely.

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the anti-bullying policy.
- All members of The Cambridge Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's policies.

4.3 Pupils use of smartwatches, personal devices and mobile phones

- Whilst situated on site at The Cambridge Primary School pupils are not permitted to wear smartwatches (a watch that has many of the features of a smartphone or a computer and a touch screen), use any personal devices or mobile phones without explicit permission from the leadership team in exceptional circumstances.

- Watches which tell the time and record step count can be worn.
- 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.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the leadership team.
- If a pupil needs to contact his/her parents/carers they will be able to do so through the school office.
- In the event that pupils bring mobile phones to school, these will be handed in at the start of the day to the school office and collected at the end of the school day. Parents will also be asked to write to the Headteacher explaining the need for a mobile phone to be brought to and from school.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers.
- Should school staff suspect that pupils have either personal devices or mobile phones on their person these may be confiscated.
- ~~Parents are not to contact their child via their mobile phone during the school day, but instead to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the headteacher.~~
- For safe use outside of school, pupils should protect their phone numbers by only giving them to trusted friends and family members.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the DSL will investigate as this becomes a Safeguarding issue.

4.4 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode and stored away during lesson times.
- Bluetooth or other forms of communication should be 'hidden' or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- If a member of staff breaches the school policy, disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school's allegations management policy.

4.5 Visitors use of personal devices and mobile phones

- Parents/carers, visitors, volunteers and work experience students, must use mobile phones and personal devices in accordance with the school acceptable use policy and as identified in the volunteer and work experience code of conduct documents.
- Use of mobile phones or personal devices by parents/carers, visitors, volunteers and work experience students to take photos or videos must be for personal use only. The owners of any photos or videos that are found to be shared through social media will be contacted by the DSL.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- The Cambridge Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team/online safety leaders will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems (by London Grid for Learning and Senso Cloud) are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school's leadership team and/or the online safety leaders.

5.2. Internet use throughout the wider school community

- The school will liaise with local schools to establish a common approach to online safety.
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure Internet use is appropriate.

5.3 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff will read and sign the Staff Behaviour (code of conduct) policy before using any school resources.
- Pupils and visitors will read and sign the Online Safety and Internet Use Agreement for Parents and Pupils before using any school resources.
- Volunteers and work experience students will read and sign the Code of Conduct documents before using any school resources.

- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Online Safety and Internet Use Agreement for Parents and Pupils (See Appendix 1) and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible Internet use amongst pupils.
- Education about safe and responsible use will precede Internet access.
- Pupils' input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Online Safety and Internet Use Agreement for Pupils and Parents (See Appendix 1) in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety will be included in the PSHE and Computing programmes of study, covering both safe school and home use.
- Online safety education and training will be included as part of the transition programme across the Key Stages and when moving between schools.
- Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety education approaches.

6.2 Engagement and education of children and young people considered to be vulnerable

- The Cambridge Primary School is aware that some children may be considered to be more vulnerable online due to a range of factors.

  The Cambridge Primary School will ensure adapted, appropriate online safety education is given with input from specialist staff as appropriate (e.g. SENCO).

6.3 Engagement and education of staff

- The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular basis.

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Members of staff with a responsibility for managing filtering systems or monitoring computing and ICT will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns (Appendix 5 and 6).
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.4 Engagement and education of parents and carers

- The Cambridge Primary School recognise that parents/carers have an essential role to play in enabling children to understand the many positives technology brings, in addition to being safe and responsible users of the Internet and digital technology.
- Parents' attention will be drawn to the school online safety policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings and transition events.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Online Safety and Internet Use Agreement for Parents and Pupils (See Appendix 1) and discuss its implications with their children.
- Information and guidance for parents on online safety (which will highlight the range of different ways children use and access technology via mobile phones, games consoles, tablets, apps, laptops, computers etc) will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Full information regarding the school's approach to data protection and information governance can be found in the school's Data Protection policy.

7.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to emails.

- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our system.
- We currently require staff to change their passwords every 3 months.

7.3 Filtering and Monitoring

- The LAC/proprietors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices as well as systems to limit children's exposure to online risks (Appendix 5 and 6).
- The school's Internet access strategy will be dependent on the need and requirements of our community and will therefore be designed (with advice from technical, educational and safeguarding staff to suit the age and curriculum requirements of our pupils).
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity which is appropriate to the age and requirement of our pupils.
- The school uses the London Grid for Learning (LGfL) WebScreen filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc where possible. SENSO Cloud software is used for network, classroom, safeguarding, monitoring and asset management.
- The school will work with LGfL to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of (Appendix 5 and 6).
- If staff or pupils discover unsuitable sites, the URL will be reported to the School DSL and/or Online Safety Leaders and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.

- All changes to the school filtering policy will be logged and recorded. This information is accessible through our filtering system with rules and dates of last modifications.
- The Leadership Team will ensure regular checks are made (through reporting) to confirm the filtering and monitoring methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Hampshire Police or CEOP (Child Exploitation and Online Protection) immediately.

LAN security issues

- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- Virus protection for the whole network must be installed and current.
- The server operating system must be secured and kept up to date.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

WAN security issues:

- HPSN2 is managed to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and HCC.

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including the sharing of nudes and semi-nudes, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, the sharing of nudes and semi-nudes, cyberbullying, illegal content etc.
- The DSL will be informed of any online safety incidents involving child protection concerns, which will then be recorded using the Online Safety Incident Reporting Log-Response Guidance (Appendix 4).
- The DSL will ensure online safety concerns are escalated and reported to relevant agencies in line with the Hampshire Safeguarding Children Partnership (HSCP) thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Complaints about online bullying will be dealt with under the school's anti-bullying policy and child-on-child abuse section of the safeguarding and child protection policy.
- Any complaint about staff misuse will be referred to the Headteacher. Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Parents are informed (through the school website) of the school's complaints procedure.
- Staff are informed of the complaints and whistleblowing procedure.
- The school's clear safeguarding vision is promoted at every opportunity (on the school website, in policies and around the school) and all member of the school community are aware of the importance of following the school's procedures for reporting concerns.

- All members of the school community are reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has, or is taking place, the school will make a referral to Hampshire Children's Services or contact Hampshire Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Hampshire Police.
- If the school is unsure how to proceed with any incidents of concern, the incident will be escalated to Hampshire Children's Services.
- If an incident of concern needs to be passed beyond the school community, the concern will be escalated to Hampshire Children's Services to communicate to other schools/settings in Hampshire.
- Parents and children will need to work in partnership with the school to resolve issues.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding the sharing of nudes and semi-nudes

- The Cambridge Primary School works to ensure all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating nude and semi-nude images.
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The Cambridge Primary School views the act of requesting, creating and sharing nudes and semi-nudes as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' and HSCP 'Responding to youth produced sexual imagery' guidance.

If the school is made aware of an incident involving youth produced sexual imagery the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Hampshire Safeguarding Children Partnership procedures.
- Immediately notify the DSL.
- Store the device securely.
- Carry out a risk assessment in relation to the children involved.
- Consider the vulnerabilities of the children involved (including carrying out relevant checks with other agencies)

- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for the children e.g. offer counselling support, immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure the school is implementing best practice.
- The leadership team will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.
- The school will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the DSL).
- The school will not send, share or save content suspected of being an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure all members of the community are aware of sources of support regarding youth produced sexual imagery.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- The Cambridge Primary School will ensure all members of the community are made aware of online child sexual abuse. This will include: exploitation, grooming and their consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The Cambridge Primary School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
- If the school is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Hampshire Children's Services and/or Hampshire Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the (Child Sexual Exploitation) CSE team, part of Hampshire Children's Services, by the DSL.
- If the school is made aware of an incident involving online child sexual abuse of a child, the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Hampshire Safeguarding Child Partnership's procedures.
    - Immediately notify the DSL.
    - Store any devices involved securely.
    - Immediately inform Hampshire Police via 101 (using 999 if a child is at immediate risk)

- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support, immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure the school is implementing best practice.
- The school leadership team will review and update any management procedures where necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted, the school will seek support from the Hampshire Children's Services to enable other schools to take appropriate action to safeguarding their community.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- The Cambridge Primary School will ensure all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent accidental access to Indecent Images of Children (IIOC) by; using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Hampshire Children's Services and/or Hampshire Police.
- If the school is made aware of Indecent Images of Children (IIOC) the school will:
  - Act in accordance with the school's child protection and safeguarding policy and the relevant Hampshire Safeguarding Child Partnership's procedures.
  - Immediately notify the school DSL.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Hampshire police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the Internet the school will:
  - Ensure the DSL is informed.

- Ensure the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure any copies that exist of the image, for example in emails, are deleted.

- If the school are made aware that indecent images of children have been found on the school's electronic devices, the school will:
  - Ensure the DSL is informed.
  - Ensure the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only. Then ensure any copies that exist of the image, for example in emails, are deleted.
- If a member of staff is found in possession of indecent images of children on their electronic device provided by the school, the school will:
  - Ensure the DSL is informed in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

- The school takes all reasonable precautions to ensure children are safe from terrorist and extremist material when accessing the Internet in school by using suitable filtering which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online, the DSL will be informed immediately and action will be taken in line with the safeguarding and child protection policy and the Prevent Duty policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed, the DSL will obtain advice immediately via Hampshire Children's Services and/or Hampshire Police.

9.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of The Cambridge Primary School community, will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All reported incidents of online bullying will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

- If the school is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Hampshire Children's Services and/or Hampshire Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include: examining school system logs; identifying and interviewing possible witnesses; and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Being asked to remove any material deemed to be inappropriate or offensive. A service provider may be contacted to remove content if those involved refuse to, or are unable to, delete content. Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's anti-bullying, behaviour policy or online safety and Internet Use Agreement for Pupils and Parents (See Appendix 1)
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

9.6. Responding to concerns regarding online hate

- Online hate at The Cambridge Primary School will not be tolerated.
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Hampshire Children's Services and/or Hampshire Police.

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

Parents are encouraged to:

- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role model safe and appropriate uses of technology and social media. This can be done in the following ways:
    - Be aware of the advice, risks and guidance surrounding online safety. This may be through reading school newsletters, information on the school website, attending the school online safety workshops or personal research.
    - Ensure children are using age appropriate apps and exposed to age appropriate content.
    - Be aware of age restrictions for social media apps and the pros and cons of children accessing them.
    - Avoid publishing any content, which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature.
    - For social networking apps (including Whatsapp) to not be used in an abusive or hateful manner.
    - To not share any personal photographs/videos taken (for example from Christmas Productions), which may include images of children other than your own, on social media without consent from both child and parent involved.
    - To only take photographs at school events with the permission of the Head Teacher. In the event that permission has been given, this will only be for personal use and not to be shared.
    - Discuss and consider consent with your child and consider the role consent plays when sharing images of your own child on your own social media platforms ('sharenting').
    - References should not be made to any staff member, pupil and parent on social media platforms, unless consent has been obtained and agreed with the individual involved.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Pupils are encouraged to:

- Develop their Computing skills and general research skills.
- Engage in online learning activities including games and quizzes.
- Develop and apply their online safety awareness and understanding of the "SMART Rules".
- Report any improper contact or cyber bullying to their class teacher in confidence as soon as it happens. We have a zero tolerance to cyber bullying.

Pupils are not permitted to:

- Download software or other files without permission (of parents and teachers).

- Send inappropriate messages or engage in inappropriate, abusive or defamatory chat and forums.
- Publish, share or distribute personal information about any user (such as home address, email address, phone numbers, photos etc).
- Use another person's login and password or allow other users to use their login and password.
- Access social networking sites during the school working day.
- Attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head Teacher. Parents will be informed if this happens.

Sanctions:

- Verbal warnings – These are given for attempts to contravene the rules. This will be followed by a written letter to parents stating what has occurred. The pupil's Internet use at school will then be monitored for a 4 week 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 Head Teacher.

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 attached school online safety rules and grant permission for my child to have access to use the Internet and other Computing facilities at school.

We have discussed the online safety rules attached to this document and my daughter or son agrees to follow the rules and to support the safe and responsible use of Computing at The Cambridge Primary School.

I accept that ultimately, the school cannot be held responsible for the nature and content of materials accessed through the Internet and devices, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, monitoring systems, restricted access, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files and the Internet sites they visit, and that if they have concerns about their online safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the Internet facilities.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

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

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

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

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

- 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 visit internet sites that are appropriate for my age.
- I will only communicate with people I know, or that a responsible adult has approved.
- I will only send polite and friendly messages.
- I will not open an attachment, or download a file, unless I have been given permission by an adult.
- I will not tell anyone my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult.

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

Parent Online Safety Agreement

As the parent or legal guardian, I have read and understood the attached school online safety rules and grant permission for my child to have access to use the Internet and other Computing facilities at school.

We have discussed the online safety rules attached to this document and my daughter or son agrees to follow the rules and to support the safe and responsible use of Computing at The Cambridge Primary School.

I accept that ultimately, the school cannot be held responsible for the nature and content of materials accessed through the Internet and devices, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, monitoring systems, restricted access, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files and the Internet sites that they visit, and that if they have concerns about their online safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the Internet facilities.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

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

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

Appendix 4: Online Safety Incident Reporting Log -Response Guidance

Online Safety Lead	Angela Beeson		
DSL DDSL	Sue Tancock (DSL) Sarah Kennedy, Vaiva Krivickiene, Fenella Holmes, Oliver Tomlinson		
Category of incident (4Cs)			
Time		Date	
Description of incident			
Name & contact details of person reporting incident			
Who was involved in the incident	child/young person staff member other (please specify)		
Names and contact details of those involved			
Type of incident (4Cs) Content Contact Conduct Commerce	Bullying or harassment Online bullying or harassment (cyberbullying) Sharing of nudes/semi-nudes (self-taken indecent imagery) deliberately Bypassing security or access hacking or virus Propagation Racist, sexist, homophobic religious hate material terrorist material other (please specify) _____		
Nature of incident	Deliberate access Accidental access		
Did the incident involve material being	Created Viewed Printed Shown to other Transmitted to others Distributed		
Could this incident be considered as	Harassment Grooming Cyberbullying Sharing of nudes/semi-nudes (self-taken indecent imagery) Breach of AUP Other (please specify) _____		

Action taken	Staff Incident reported to head teacher/senior manager Advice sought from children's social care Incident reported to police Incident reported to CEOP incident reported to Internet Watch Foundation Incident reported to IT Disciplinary action to be taken Online policy to be reviewed/amended Child/young person Incident reported to member of staff (specify) _____ Incident reported to social networking site incident reported to IT Child's parents informed Disciplinary action taken child/young person debriefed Online Safety Policy to be reviewed/amended

Outcome of incident/ investigation

Children's social care	
Police/CEOP	
Organisation	
Individual (staff member/child)	
Other (HR/legal etc)	
Children's social care	

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 2023 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) 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.
- A weekly report is run by Sue Tancock every Friday and logged in the following location - S:\Safeguarding\Filtering & Monitoring\Filtering & Monitoring Reports\2023-24

- 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 is 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) is responsible for testing the filtering system on a termly basis.

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.

Contact **Sue Tancock** 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 **Sue Tancock** as soon as possible, or please speak to any member of the DSL Team.

Appendix 6: How CPS meet the Filtering and Monitoring Standards for Schools and Colleges

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.