Thameside Primary School: E Safety Policy

Approved by Governors: April 2023

Review date: March 2024

Contents

Policy reviewed by:	Becky Fidgett
Key Changes:	1.1 added in fourth 'C' – commerce 1.2 changed lead name and added Kent County Council's new name 1.3.1 added annual online safety training to 7th bullet point 3.4 Added in bullet point about social media minimum age 4.4 changed bullet points about using personal devices to contact families 6.1 specified when online safety will be taught Appendix B – specified where phones are to be handed in and stored (Y6 – in classroom, Y5 – in office), added record to second bullet point in second section Appendix D – updated links and removed inactive links Added Appendix E – how to hide caller ID Added Appendix F – Social media minimum ages

Rights Respecting Schools

Thameside Primary School is a Rights Respecting School. School policies will respect the UN Convention on the Rights of the Child. The online safety policy links to:

Article 17: *Children have the right to get information from the mass media. Radio, television, newspapers and the internet should provide information that children can understand and not promote materials that could harm children.*

Keeping Children Safe in Education states: *It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.*

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

Thameside Primary School believes that online safety (e-safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. We identify 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. Thameside 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. We identify that there is a clear duty to ensure that all children and staff are protected from potential harm online, including all four C's: **content** shared online, **contact** from others, **conduct** of your behaviour and financial risks of **commerce**.

The purpose of Thameside 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 to ensure that Thameside Primary School is a safe and secure environment and protects from the four C's.
- Safeguard and protect all members of the Thameside school community online.
- Raise awareness with all members of the Thameside school community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to 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 governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school 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 work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies such as Safeguarding and Child Protection, Anti-bullying, Whistleblowing, Keeping Children Safe in Education and Behaviour.

1.2 Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSLs) is Mrs S Greenaway. This is not a technical role.

The Online Safety policy has been written by the Computing Leader, Mrs B Fidgett, building on the Kent County Council's Online Safety Policy (now The Education People) and government guidance. It has been agreed by senior management and approved by governors.

1.3 Key responsibilities for the community

1.3.1 The key responsibilities of the school management and leadership (SLT) 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, including working alongside the computing co-ordinator to ensure participation in local and national events to promote positive behaviour, e.g. Safer Internet Day.
- Supporting the DSLs by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Liaising with DSLs to ensure there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- 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 e.g: CPD Purple Mash training and annual online safety training.
- 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 and the associated risks and safe 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/monitoring online safeguarding records and online safety incidents/concerns 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 (e.g. CEOP and IWF).
- 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 Governing Body is identified with a lead responsibility for supporting online safety – at Thameside, this is covered within the role of our nominated Safeguarding Governor.

1.3.2 The key responsibilities of the DSLs are (in addition to those of SLT):

- Acting as a named point of contact for 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.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitor the school online safety incidents to identify gaps/trends and use this data to update the school education response to reflect need.
- To report to the school management team, Governing Body and other agencies as appropriate on online safety concerns and local data/figures.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies and adhering to them. In July of Year 2, teachers must ensure children read, understand and sign the KS2 Acceptable Use Policy and this should then be stored in their blue folders in the school office.
- 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 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.
- Reporting any e-safety concerns of children in their care via CPOMS and alerting the DSLs.
- Completing the e-safety incident report form (appendix A), scanning in to CPOMS and placing the hard copy in Head teachers' office if an incident of concern online happens during a lesson.
- Being able to signpost appropriate support available for online safety issues, internally and externally (e.g. CEOP and IWF).
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment and ICT co-ordinators are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are maximised.
- Taking responsibility for the implementation of security of 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 DSLs.
- Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSLs.
- Report any breaches and concerns to the DSLs 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 DSLs and leadership team, especially in the development and implantation of appropriate online safety policies and procedures.

1.3.5 The key responsibilities of children and young people are:

- Contributing to the development of online safety procedures.
- Reading the school's Acceptable Use Policies and adhering to them.
    - When children join Thameside Primary, in EYFS, they will complete the KS1 version of the policy.
    - At the end of Year 2 (in July) children will read and sign the KS2 Acceptable Use Policy; this will form part of their transition into KS2.
- 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.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- 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.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school's Acceptable Use Policies, 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.
- 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, or other appropriate agencies, if they or their child encounters online problems or concerns.

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department of Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

- The website with the school's guidelines for publications including accessibility, respect for intellectual property rights, privacy policies and copyright.

2.2. Photographing children (taken from p.31 of our Safeguarding & Child Protection Policy)

- We understand that parents like to take photos of or video record their children in the school play, or at sports day, or school presentations. This is a normal part of family life, and we will not discourage parents from celebrating their child's successes. However, if there are Health and Safety issues associated with this - i.e. the use of a flash when taking photos could distract or dazzle the child, we will ask that flash photography is disabled.
- We will not allow images of pupils to be used on school websites, publicity, or press releases, without express permission from the parent, and if we do obtain such permission, we will not identify individual children by name. All parents will be asked for written permission to use photos as required by GDPR.
- The school cannot however be held accountable for photographs or video footage taken by parents or members of the public at school functions although we will ask parents not to put photos of other children on social networking sites

2.3 Publishing images and videos online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy and with parental/carer consent.
- The school will ensure that all use of images and videos take place in accordance with other policies and procedures including data security, Acceptable Use Policies, Codes of Conducts, social media, use of personal devices, Keeping Children Safe in Education and mobile phones, etc.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published

2.4 Managing email

- Pupils may only use school provided email accounts for educational purposes.
- All relevant members of staff are provided with a specific school email address to use for any official communication.
- 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 email systems will always take place in accordance to General Data Protection Regulation 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 records.

2.5 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 will be designed to enhance and extend education, sharing appropriate **content** online with the children.
- 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 in order to ensure the **content** children see online is appropriate.
- All school owned devices will be used in accordance with the school's Acceptable Use Policy and with appropriate safety and security measures in place.
- 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 in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- 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.

Supervision of pupils will be appropriate to their age and ability:

- At Foundation Stage and Key Stage One, pupils' access to the internet will be by adult demonstration with occasional directed supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
- At Key Stage Two, pupils will be supervised. 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.

3. Social Media Policy

3.1 General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the Thameside community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the Thameside community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the Thameside community.
- All members of the Thameside community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Any concerns regarding the online conduct of any member of the Thameside community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with the relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

Thameside Primary School's official social media channels are:

- Facebook - https://www.facebook.com/Thameside-Primary-School-1237080259660697/

- Twitter - https://twitter.com/ThamesideSch

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the head teacher.
- Official school social media channels will be set up as a distinct and dedicated social media site for educational or engagement purposes.

- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy to ensure they are aware of the required behaviours and agree to **conduct** themselves in the manner established in the policy. They are required to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media sites will be clear, transparent and open to scrutiny.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Any online publication on official social media sites will comply with legal requirements including the General Data Protection Regulation 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites in accordance with the image use policy and parent/carer consent. Staff with check each child's consent form before posting.
- Information about the safe and responsible use of social media channels will be communicated regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run from and/or linked to the school website and take place with approval from the Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and the head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.

3.3 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy
- All members of staff are advised not to communicate or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Designated Safeguarding Lead and/or head teacher.
- If ongoing **contact** with pupils is required once they have left the school roll, then members of staff will be expected to use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- Staff will not use personal social media accounts to make **contact** with pupils in any circumstances. Staff are strongly advised not to use personal social media accounts to make contact with parents. If they do, professional judgement, caution and integrity MUST be used.
- Any communication from pupils/parents received on personal social media accounts will be reported to the Designated Safeguarding Lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting their privacy levels of their personal sites as strictly as they can, opting out of public listings on social media sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the leadership team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- School email addresses will not be used for setting up personal social media accounts.

3.4 Pupil use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.

- Children and parents should be reminded that the minimum age for most social media sites is 13 years old (see Appendix F for minimum ages)
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to have **contact** with those they have not met in person, advising that they do not meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present. Children will be advised of what to do in lessons if they were **contacted** by someone they do not know – for more information please see section 6.1.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and confidential passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Any official social media activity involving pupils will be moderated by the school where possible.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

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 Thameside 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 covered in appropriate policies including the school Acceptable Use agreement. Thameside Primary School recognised 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 and appropriately within school.

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.

- No electronic devices or personal devices other than mobile phones should be brought onto the school site. Mobile phones that are brought on site are the responsibility of the user at all times.
- Pupils' mobile phones are not permitted to be used on the school site and must be handed in to the school office on arrival. They are not allowed to be taken by pupils on school trips, including residential stays. The only exception to this is children who may require their mobile phone to control and monitor their diabetes, for example.
- 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 on the school site will be dealt with as part of the behaviour policy.
- All members of the Thameside community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage, e.g. storing them in a locker.
- All members of the Thameside community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

4.3 School rules for the acceptable use of a mobile phone in school by primary pupils

- Reception to Year 4 pupils are forbidden from bringing a personal mobile phone to school. If a child in these year groups brings a phone to school the agreed procedure is that this will be handed over to a member of staff who will send it to the office for safe keeping during the day. This can then be collected at the end of the day from the office by a parent. If a child in these year groups has a specific reason parents deem them to need a mobile phone in school, permission must be granted from the head teacher.
- Parents will be informed by the school website and this policy that the school will not be held responsible for the security of a mobile phone brought into school unless they are handed to staff for safekeeping.
- Pupils in Year 5 and 6 are permitted to bring a mobile phone to school, to support safety issues if they come to school independently. All mobile phones should be named and handed to the office at the start of the school day for safe keeping and collected back at the end of the day. They must sign the Mobile Phone Acceptable Use Agreement (see appendix B).

4.4 Staff use of personal devices and mobile phones

- Members of staff should not use their own personal phones or devices for contacting children and young people within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with team leaders and/or the head teacher.

- Members of staff should only use their own personal phones or devices for contacting children's families when deemed absolutely necessary e.g. virtual parents' evenings or school trips. If they are doing so, they need to ensure that their caller ID is hidden (see Appendix E on how to do this)
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will 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 will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable use, etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

4.5 Visitor use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school Acceptable Use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

5. Policy Decisions

5.1 Reducing online risks

- Thameside 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 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 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.

5.2. 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 through use of usernames and passwords kept by the school technician.
- All staff and pupils will read and sign the Acceptable Use Policy before using any school resources. Visitors will be given the safeguarding leaflet to read on arrival.
- 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 Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as children with special educational needs) the school will make decisions based on specific needs and understanding of the pupils.

6. Engagement Approaches

6.1. Engagement and education of children

- An online safety (e-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. This will be taught through the schools e-learning software at the beginning of each academic year: Purple Mash, around Safer Internet Day and as part of PSCHE.
- Purple Mash holds many resources and lessons plans to engage children in learning about the importance of staying safe online. Purple Mash was cross-checked against the key areas the government wish to include in schools e-safety learning. See Appendix C for this information.
- 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 Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety (e-safety) will be included in the PSCHE, SRE and Computing programmes of study, covering both safe school and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

6.2 Engagement and education of children considered to be vulnerable

- Thameside Primary School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- Thameside Primary School will ensure that differentiated and ability appropriate online safety (e-safety) education is given, with input from specialist staff as appropriate

6.3 Engagement and education of staff

- The online safety (e-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 the school's 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 (at least annual) 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.

6.4 Engagement and education of parents and carers

- Thameside Primary School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats, such as on the school website, through parent workshops and curriculum letters, etc.
- 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 General Data Protection Regulation 2018.
- Full information regarding the school's approach to data protection and information governance can be found in the school's information security 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.
- Files held on the school's network will be regularly checked.
- The ICT Technician, John, will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.

7.3 Password Policy

- All users will be educated not to share their computer login passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep login passwords private and must not share them with others.
- Pupils' passwords to online education sites are located in the front of their personal reading records (to use in lessons and/or at home) and accidental login to these sites by other children does not mean that they would have access to any sensitive personal data.
- 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.
- From Year 3, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system e.g. at least 8 characters long and including a mixture of both uppercase letters, lowercase letters and numbers.
- We require staff to change their passwords regularly in line with advice from the ICT Technician.

7.4 Filtering and Monitoring

Named lead: Mrs Sophie Greenaway

- The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

- 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 through RM-SafetyNet which is appropriate to the age and requirement of our pupils.
- The school uses RM-SafetyNet's filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will ensure that we are in line with the UK Safer Internet Centres published guidance as to what 'appropriate' filtering looks like. https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring
- The school will work with RM- SafetyNet to ensure that filtering policy is continually reviewed.
- Filtering breaches are reported by staff to the Head teacher (also DSLs) and ICT technician and Computer lead. Children will report any filtering breaches to their teachers.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead 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.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Thames Valley Police or CEOP immediately.

7.5 Management of applications used to record children's progress

- The head teacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.

- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the school expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

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 sexting, 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 (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content, etc.
- The Designated Safeguarding Lead will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Reading Local Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the school's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaint procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be 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 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 taken place or is taking place then the school will contact the Reading Local Safeguarding Children Board or Thames Valley 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 Thames Valley Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Reading Local Safeguarding Children Board.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Reading Local Safeguarding Children Board to communicate to other schools in Reading.
- 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 in concerns regarding Youth Produced Sexual Imagery or "Sexting"

- Thameside Primary School ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting")
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Thameside Primary School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead, Sophie Greenaway.
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people and KSCB 'Responding to youth produced sexual imagery' guidance.

If the school are made aware of any incidents involving creating youth produced sexual imagery, the school will:

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

- Make a referral to children's social care and/or the police (as appropriate).
- Put the necessary safeguards in place for children.
- 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 that the school is implementing best practice and 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 an image 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 Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be 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 then 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 that 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

- Thameside Primary School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming, the 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 appropriate educational approaches for pupils, staff and parents/carers.
- Thameside Primary School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead, Sophie Greenaway (headteacher).
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Reading Local Safeguarding Children Board and/or Thames Valley Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through the CSET team or social services by the Designated Safeguarding Lead.
- If the school are made aware of an incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Reading Local Safeguarding Children Board's procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store any devices involved securely.
- Immediately inform Thames Valley 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).
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and 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 then the school will seek support from the Reading Local Safeguarding Children Board to enable other schools to take appropriate action to safeguard their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button on the school website homepage and on intranet systems.

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

- Thameside Primary School will ensure that 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 access and accidental access to Indecent Images of Children (IIOC), for example 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 then the Designated Safeguarding Lead will obtain advice through the Reading Local Safeguarding Children Board and/or Thames Valley Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Reading Local Safeguarding Children Board's procedures.
    - Immediately notify the school's Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Thames Valley 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, then the school will:
    - Ensure that the Designated Safeguarding Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school is made aware that indecent images of children have been found on the school's electronic devices, then the school will:
    - Ensure that the Designated Safeguarding Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform Thames Valley Police via 101 (using 999 is a child is at immediate risk) 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.
- If the school is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
    - Ensure that the Designed Safeguarding Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact Thames Valley 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 will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the safeguarding 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 then the Designated Safeguarding Lead will obtain advice immediately via the Reading Local Safeguarding Children Board and/or Thames Valley Police.

9.5 Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the Thameside community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported 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 then the Designated Safeguarding Lead will obtain advice immediately through the Reading Local Safeguarding Children Board and/or Thames Valley 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 online safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be 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 or acceptable use policies.
- The police will be contacted if a criminal offence is suspected.

9.6 Responding to concerns regarding online hate

- Online hate at Thameside Primary School will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online hate reported to the school will be recorded.
- All member of the community will be advised to report online hate in accordance with relevant school policies and procedures, for example 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 then the Designated Safeguarding Lead will obtain advice immediately through the Reading Local Safeguarding Children Board and/or Thames Valley Police.

Appendix A

E safety Incident Report Form

Name of school:		
Your details		
Your name:	Your position:	Date and time of incident:
Details of e-safety incident		
Date and time of incident:		
Where did the incident occur? i.e. at school or at home:		
Who was involved in the incident? Child/young person ☐ Name of child…… Staff member/ volunteer ☐ Name of staff member/ volunteer…… Other ☐ please specify……		
Description of incident:		

Action taken:

- ☐ Incident reported to head teacher/senior manager
- ☐ Advice sought from Safeguarding and Social Care
- ☐ Referral made to Safeguarding and Social Care
- ☐ Incident reported to police
- ☐ Incident reported to Internet Watch Foundation
- ☐ Incident reported to IT
- ☐ Disciplinary action to be taken
- ☐ E-safety policy to be reviewed/amended
- ☐ Other (please specify) .....

Outcome of investigation:

NSPCC
Cruelty to children must stop. FULL STOP.

Appendix B

Acceptable Use of Mobile Phones Agreement

Expectations for safe use of personal devices and mobile phones:

- Pupils in Year 5 and 6 are permitted to bring a mobile phone to school, to support safety issues especially if they travel to and from school independently.
- Pupils' mobile phones are not permitted to be used on the school site.
- In Year 5, all mobile phones should be named and handed to the office at the start of the school day for safekeeping and collected back at the end of the day.
- In Year 6, all mobile phones should be named and handed to a member of Year 6 staff at the start of the school day for safekeeping and collected back at the end of the day.

If parents want their child to bring a phone to school, it is on the understanding that they agree with the following limitations on use, namely:

- Mobile phones must be switched off at all times during the school day, including break and lunchtimes.
- It is not permitted to film, photograph or record anyone on school grounds.
- The phone will be kept in the office store cupboard or the Year 6 lockers during the day.
- The school will not be held responsible for the security of a mobile phone brought into school.
- The school reserves the right not to allow a pupil to bring their phone on to the school site if its use by the pupil is deemed to be unacceptable.

The school will consider any of the following unacceptable use of the mobile phone and a serious breach of the school's behaviour policy and this agreement:

- Photographing or filming staff of other pupils during the school day and on organised school events
- Photographing or filming in toilets, swimming pools, changing rooms and similar areas
- Bullying, harassing or intimidating staff or pupils by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites
- Refusing to switch a phone off or hand over the phone at the request of a member of staff#
- Using the mobile phone outside school hours to intimidate or upset staff and pupils will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time

I agree to follow these limitations on use and consequences of misuse.

Name of pupil…… Date…….

Mobile phone number of pupil ……

Signed (parent)……. Signed (pupil)…….

Appendix C

8 things the government wants schools to teach about online safety vs Purple Mash curriculum

Yellow team scheme Green team scheme Blue team scheme

1. **Spotting fake news**
    - Scheme in Year 3 looks into spoof websites – thinking critically about the websites and the results returned to a search
    - Learning about phishing
    - Considering if the news from searches is reliable
    - References sources in their work
    - Search the Internet with a consideration for the reliability of the results
    - Looking for privacy seals of approval
2. **Social media influencers**
    - Upsetting videos
    - To understand the advantages, disadvantages, permissions and purposes of altering an image digitally and the reasons for this.
    - Social network debate (app)
    - Friendbook (app)
3. **Dangers of online challenges**
    - Ok to say no section
    - Meaning of age restrictions online
    - To review sources of support when using technology.
    - To have a clear idea of appropriate online behaviour and how this can protect themselves
4. **How to limit personal data 'harvesting'**
    - **Importance of passwords and keeping information safe**
    - **Introduce the idea of 'ownership' of their creative work**
    - **Digital footprint**
    - **Importance and learn how to keep information safe and secure**
    - **Learning about phishing**
    - **Identify theft**
    - **Maintain secure passwords**
5. **That porn is not an 'accurate portrayal' of sexual relationships**
    - **Not covered on the schemes that I can see – will email them and find out more.**
    - **Maybe needs to be edited into our new RSHE schemes for year 5/6.**
6. **The risks of live streaming**

- To be aware of appropriate and inappropriate text, photographs and videos and the impact of sharing these online.
- To have a clear idea of appropriate online behaviour and how this can protect themselves

7. **How 'online emotions' can result in 'mob mentality'**
    - To be aware of appropriate and inappropriate text, photographs and videos and the impact of sharing these online.
    - Children understand how what they share impacts upon themselves and upon **others** in the long-term.
    - Children know about the consequences of promoting inappropriate content online and how to put a stop to such behaviour when they experience it or witness it as a bystander.
8. **Knowing the different types of grooming**
    - To have a clear idea of appropriate online behaviour and how this can protect themselves (on the website this advises being covered in RSHE lessons)

Appendix D

Online Safety (e-safety) Contacts and References

National Links and Resources

Action Fraud: https://www.actionfraud.police.uk/

BBC WebWise: https://www.bbc.co.uk/programmes/p023xv3k

CEOP (Child Exploitation and Online Protection Centre): https://www.ceop.police.uk/Safety-Centre/

ChildLine: https://www.childline.org.uk/

Childnet: https://www.childnet.com/

Family Online Safe: https://www.fosi.org/

Get Safe Online: https://www.getsafeonline.org/

Internet Matters: https://www.internetmatters.org/

Internet Watch Foundation (IWF): https://www.iwf.org.uk/

Lucy Faithfull Foundation: https://www.lucyfaithfull.org.uk/

NSPCC: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

The Prevent Duty: https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

UK Council for Internet Safety: https://www.gov.uk/government/organisations/uk-council-for-internet-safety

South West Grid for Learning: https://swgfl.org.uk/

The Marie Collins Foundation: https://www.mariecollinsfoundation.org.uk/

Think U Know: https://www.thinkuknow.co.uk/

Virtual Global Taskforce: https://nationalcrimeagency.gov.uk/virtual-global-taskforce/

UK Safer Internet Centre: https://saferinternet.org.uk/

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Appendix E

How to hide caller ID

On iPhones:

1. Open Settings. Unlock your iPhone and find the Settings app, it is grey and looks like cogs.
2. Click on Phone. Scroll down in your Settings and click on the button that says Phone, which has a small, green phone logo next to it.
3. Go to Show My Caller ID and click on it. ...
4. Turn it off.

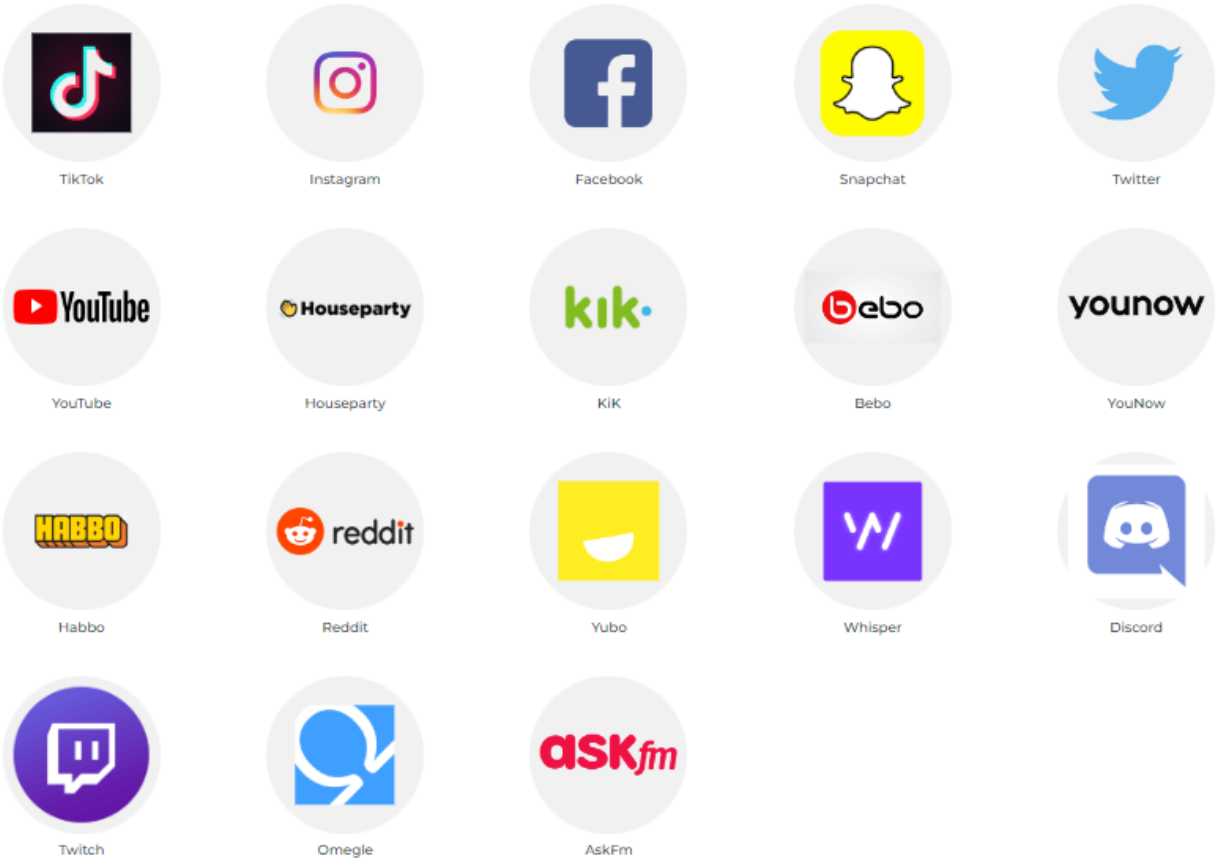
On Android:

1. Open the Phone app, and open the Menu.
2. Select Settings, then Call settings.
3. Click on Additional settings, then Caller ID.
4. Choose “Hide number” and your number will be hidden.

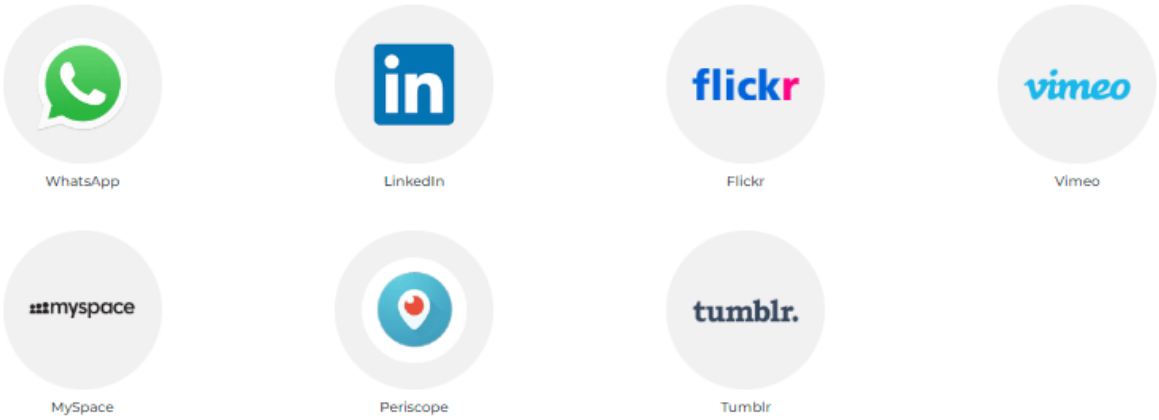
Appendix F

Social Media Minimum Ages

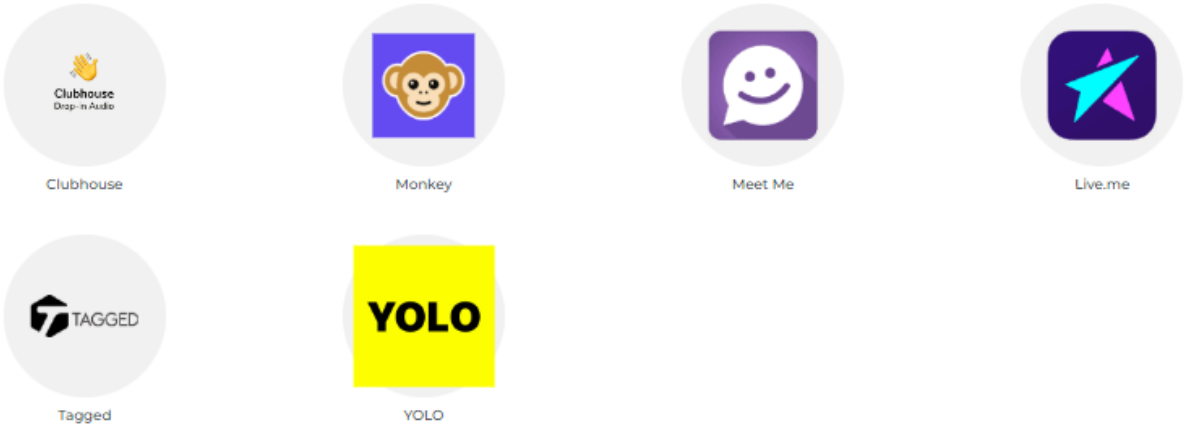
13 year olds and upwards



16 year olds and upwards



Not suitable for under 18 year olds



Screenshots taken from https://www.internetmatters.org/resources/what-age-can-my-child-start-social-networking/