ICT and E-Safety Policy: Cyberbullying and Social Media

1.0 Introduction 3
1.1 Use of this policy 3
2.0 Managing Access and Security 4
3.0 Internet Use 4
3.1 Students Use of IT Systems 4
3.2 Learning to Evaluate Internet Content 5
4.0 E-mail 5
5.0 Published content 5
6.0 Use of Social Media 5
6.1 Use of Generative Artificial Intelligence (AI) 6
7.0 Use of Personal Devices 6
8.0 Taking, Storing and Publishing Images of Children (see also Code of Conduct for Staff) 7
9.0 Policy Decisions Authorising Access 7
10.0 Assessing Risks 7
11.0 Handling E-Safety Complaints 8
12.0 E-Safety and Safeguarding 8
12.1 Cyberbullying 8
12.2 Radicalisation and the Use of Social Media to Encourage Extremism 9
12.3 ICT based sexual abuse 9
12.4 Chat Room Grooming and Offline Abuse 9
12.5 Harmful Sexual Behaviour and Sexual Violence 9
12.6 Online Learning 10
12.7 Modern Slavery and Financial Exploitation 11
12.8 Supporting Vulnerable Groups Online 11
13.0 Community Use of the Internet 12
14.0 Communication of the Policy 12
Appendix 1: Online Safety – Areas of Risk 14
Appendix 2: Roles and Responsibilities 16
Appendix 3: Reporting of E-Safety Issues and Concerns Including Concerns Regarding Radicalisation 17

Key References: In addition to this policy Cobham Montessori School takes due regard for, and refers to, and additional details found in the following DfE publications:

The Equality Act, 2010

SEND Code of Practice, 2014

Keeping Children Safe in Education

Teaching Online Safety in School

Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Guidance for Practitioners

Education for a Connected World 2020

Behaviour and Discipline in Schools, February 2024

Preventing and Tackling Bullying Advice, July 2017

How Social Media is Used to Encourage Travel to Syria and Iraq

Data Protection Act 2018

https://www.legislation.gov.uk/ukpga/2025/18/contents

Links are current as of September 2026

For further information please refer to our full policy list for related policies.

1.0 Introduction

This policy covers all pupils in the school, including those in the Children's House and Elementary. E-safety is part of the school's safeguarding responsibilities. This policy recognises the age, appropriate digital skills and competencies which children need to develop as described in the Education for a Connected World Framework. This policy informs and supports a number of other school policies, including our Safeguarding and Child Protection Policy which incorporates our guidance on Preventing Extremism and Radicalisation. All staff should read these policies in conjunction with the E-Safety Policy. This is particularly important with regard to the Prevent strategy, as a large portion of cases of radicalisation happen through the online medium

1.1 Use of this policy

The person responsible for overseeing E-Safety at Cobham Montessori School is Shona Dolan with Yvonne Cooke as Prevent Officer and DSL. See Appendix 2 for further details on the role of the E-Safety officer.

- Our E-Safety Policy has been written by the school, building on best practice and government guidance.
- The E-safety policy is to be revised annually or when changes in legislation are released.
- The E-Safety policy covers the use of all technology which can access the school network and the internet, or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets, smart watches and hand-held games consoles used on the school site.
- The E-Safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil

- The E-Safety policy acknowledges the Home Office/DFE document 'How Social Media is Used to Encourage Travel to Syria and Iraq - Briefing Note to School'

2.0 Managing Access and Security

The school provides managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school uses a recognised internet service provider - at present Talk Talk.
- The school has an internet filtering system provided by Talk Talk. This system provider is flexible to block different sites for different groups of children and adults. We are also able to block any sites which may encourage radicalisation. This is regularly checked to ensure that it is working, effective and reasonable using https://swgfl.org.uk/services/test-filtering/
- **The school's filtering and monitoring systems are reviewed at least once every academic year by the Senior Leadership Team member responsible for filtering and monitoring (Shona Dolan), supported by the Designated Safeguarding Lead (Yvonne Cooke) and our IT support provider (Talk Talk). These reviews are documented and retained as evidence of compliance.**
- The school ensures that its networks have virus and anti-spam protection.
- Access to school networks is controlled by personal passwords.
- Use of the internet is monitored, and a log of any incidents kept to help to identify patterns of behaviour and to inform E-safety policy.
- The security of school IT systems are reviewed regularly.
- All staff have clear procedures for reporting issues. See Appendix 3: Responding to an E-Safety incident.
- The school ensures that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

using https://swgfl.org.uk/services/test-filtering/

3.0 Internet Use

The school provides an age-appropriate E-Safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. All communication between staff and pupils or families takes place using school equipment and/or school accounts. Pupils are advised not to give out personal details or information which may identify them or their location.

3.1 Students Use of IT Systems

All students must agree to the IT Acceptable Use Policy (AUP) before accessing the school systems. Students at Cobham Montessori School are given supervised access to our computing facilities and are provided with access to filtered Internet. The promotion of online safety within ICT activities is considered essential for meeting the learning and development needs of children. The school will ensure that the use of Internet derived materials by staff and Students complies with copyright law.

Cobham Montessori School will help children to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our PSHE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (https://www.thinkuknow.co.uk/)

3.2 Learning to Evaluate Internet Content

With so much information available online, it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. "fake news");
- about the risks associated with using the internet and how to protect themselves and their peers from potential risks;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

4.0 E-mail

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- At present pupils do not use personal emails. Under direct supervision they may be supported to send an email from the school's elementary account.

5.0 Published content

This refers to; for example: school web site, school social media accounts.

- The contact details are the school address, email, and telephone number. Staff or pupils' personal information are not published.
- The website manager has overall editorial responsibility and ensure that content is accurate and appropriate.

6.0 Use of Social Media

- The school has a separate social media policy described in the Code of Conduct for Staff. The school will control access to social networking sites and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype or Zoom is monitored by staff. Pupils do not use this without full supervision by a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in school and out, takes into account the feelings of others and is appropriate for their situation as a member of the school community.

6.1 Use of Generative Artificial Intelligence (AI)
Cobham Montessori School recognises that Generative AI tools are increasingly being used in educational settings and present both opportunities and risks for safeguarding, data protection, and ethical use.
Staff Use of AI:

- Staff may use AI tools for educational purposes only when such use has been approved by the Head of School and complies with our data protection obligations under the Data Protection Act 2018, UK GDPR, and Data (Use and Access) Act 2025.
- Staff must not input any personal data about pupils, families, or other staff members into AI tools unless the tool has been specifically approved for this purpose and appropriate data protection safeguards are in place.
- Staff must critically evaluate all AI-generated content before using it with pupils or sharing it with the school community.
- Staff should model responsible AI use and be transparent with pupils when AI tools have been used.

Pupil Use of AI:

- Pupils may only use AI tools under direct staff supervision and when it forms part of a planned educational activity.
- Pupils will be taught about AI as part of our E-Safety and digital literacy curriculum, including:
    - What AI is and how it works
    - The limitations and potential biases of AI-generated content
    - How to identify AI-generated content
    - The importance of critical thinking when using AI tools
    - Ethical considerations around AI use

Safeguarding Risks Associated with AI: The school recognises specific safeguarding risks associated with AI, including:

- **Deepfakes and digitally altered images:** AI can be used to create realistic but fake images, videos, or audio recordings. This includes the creation of indecent images of children using AI technology, which is a criminal offence.
- **AI-generated harmful content:** AI tools may generate inappropriate, harmful, or inaccurate content.
- **Privacy violations:** AI tools may collect, store, or share personal data inappropriately.

All incidents involving AI-generated harmful content, including deepfakes or AI-generated indecent images, will be treated as serious safeguarding concerns and managed in accordance with our Safeguarding and Child Protection Policy.
Review of AI Use: The use of AI tools in school will be reviewed termly by the E-Safety Officer and DSL as part of our safeguarding review, to ensure that emerging risks are identified and managed appropriately.

7.0 Use of Personal Devices

- Personal equipment (such as laptops) may be used by staff to access the school IT systems provided their use complies with the E-Safety policy, data protection policy and staff code of conduct.
- Use of personal devices is clarified in the Staff Code of Conduct.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.
- Cobham Montessori School operates as a mobile phone-free environment. Children must not bring or use their own mobile technology in school at any time, including during lessons, breaktimes, and lunchtimes. This restriction applies to all mobile phones, smart watches, tablets, and other personal devices capable of internet access or communication.
- Any exceptions to this policy (for example, for specific medical or safeguarding reasons) must be agreed in advance with the Head of School and documented in writing.

8.0 Taking, Storing and Publishing Images of Children (see also Code of Conduct for Staff)

Written permission is obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media.

Cobham Montessori School provides an environment in which children, parents and staff are safe from images or audio being inappropriately recorded or used. This prevents staff from being distracted from their work with children and ensures the safeguarding of children from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere on the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a mobile phone policy included in our Code of Conduct for Staff: Visitors are advised of the restrictions regarding us of mobile phones on entry to the school.

9.0 Policy Decisions Authorising Access

- All staff (including teaching assistants, support staff, office staff, student teachers, work experience trainees) must read the acceptable use policy before accessing the school IT systems.
- The school maintains a current record of all staff and pupils who are granted access to school IT systems.
- In the Children's House, access to the internet is by adult demonstration with very occasional fully supervised access to specific, approved on-line materials.
- In the Elementary access to the internet is with teacher permission with increasing levels of autonomy appropriate to the level of maturity of the child. See Appendix 2
- People not employed by the school must read the Adult AUP before being given access to the internet via school equipment.
- Parents are asked to sign and return their child's AUP - a consent form to allow use of technology by their pupil.

10.0 Assessing Risks

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

- Technologies such as personal smartphones with internet access are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed. Such smartphones are not allowed to be used for school related matters.
- We will audit ICT use to establish if the E-Safety policy is sufficiently robust and that the implementation of the E-Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed termly with the DSL as part of the Safeguarding review.
- Emerging technologies will be examined by the Head of School for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *wifi* access.

11.0 Handling E-Safety Complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection/safeguarding procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's Behaviour Policy.

12.0 E-Safety and Safeguarding

12.1 Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously. The anonymity that can come with using the internet can sometimes make people feel safe to say and do things that they would otherwise would not do in person. It is made clear to all members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

There are multiple methods of cyberbullying using a variety of channels including mobile phones, tablets, laptops and other devices connected to the internet. The following are all considered cyberbullying and will be treated as such.

1. Exclusion – the deliberate act of leaving someone out.
2. Harassment - a sustained, constant and intentional form of bullying comprising abusive or threatening messages sent to your child or to a group.
3. Outing - a deliberate act to embarrass or publicly humiliate someone through the online posting of sensitive, private or embarrassing information without their consent.
4. Cyberstalking – can refer to children or adults contacting or threatening the physical or mental wellbeing or safety of another person.
5. Fraping – the act of impersonating someone online using their social media accounts.
6. Fake Profiles – to hide one's identity in order to carry out cyberbullying activity.
7. Dissing - the act of sending or posting cruel information about someone online, to damage their reputation or friendships with others
8. Trickery - the act of gaining someone's trust so that they reveal secrets or embarrassing information that the cyberbully then shares publicly online.

9. Trolling - the deliberate act of provoking a response through the use of insults or bad language on online forums and social networking sites.
10. Catfishing - when another person steals your online identity, usually photos, and re-creates social networking profiles for deceptive purposes.

Any incidents of cyberbullying will be dealt with in accordance with the school's Behaviour Policy, Anti-Bullying Policy and, where appropriate, the school's Safeguarding Policies and procedures.

12.2 Radicalisation and the Use of Social Media to Encourage Extremism

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- confirming extreme beliefs;
- accessing to likeminded people where they are not able to do this off-line, creating an online community;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Cobham Montessori School has a number of measures in place to help prevent the use of Social Media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by Students.
- Students, Parents and Staff are educated in safe use of Social Media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '[How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.]'

12.3 ICT based sexual abuse

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. All adults (volunteers, staff) working with students, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

12.4 Chat Room Grooming and Offline Abuse

Our staff will need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of students online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

12.5 Harmful Sexual Behaviour and Sexual Violence

Cobham Montessori School recognises that children can abuse their peers in a sexual way, and that such behaviour exists on a continuum from harmful sexual behaviour (HSB) to sexual violence.

Understanding Harmful Sexual Behaviour: Harmful sexual behaviour (HSB) refers to sexual behaviour displayed by children that is developmentally inappropriate, may be harmful towards self or others, or be abusive towards another child or adult. HSB can occur online as well as offline.

We recognise that:

- Not all harmful sexual behaviour is abusive or violent
- Some sexual behaviour between children is part of normal development, while other behaviour may indicate a safeguarding concern
- The NSPCC provides guidance on typical stages of sexual development to help staff identify when behaviour may be concerning

Online Harmful Sexual Behaviour and Sexual Harassment: Sexual harassment and harmful sexual behaviour is not tolerated at Cobham Montessori School. We recognise that sexual harassment can take place online including:

- **Making or sharing of nudes or semi-nudes (including images and/or videos)** - this includes consensual and non-consensual sharing and is a criminal offence
- **Images that are digitally altered or wholly generated by artificial intelligence (such as deepfakes)** - all such incidents mandate a safeguarding response
- Upskirting (a criminal offence)
- Sharing of unwanted explicit content
- Sexualised online bullying
- Sexual exploitation and coercion

Understanding Consent: Age-appropriate education about consent is integrated into our SMSC and PSHE curriculum. We teach pupils that:

- Consent must be freely given, informed, and ongoing
- Consent can be withdrawn at any time
- A person cannot give consent if they are under the influence of substances, asleep, or lack capacity
- Consent to one activity does not mean consent to another

Response to Incidents: All incidents of harmful sexual behaviour, sexual harassment, or sexual violence (whether online or offline) will be taken seriously and managed in accordance with our Safeguarding and Child Protection Policy and Part Five of Keeping Children Safe in Education 2026.

The E-safety, SMSC and PSHE curriculums aim to inform the students in an age-appropriate way about suitable behaviour, healthy relationships, and consent. Newsletter updates with current E-Safety information aim to educate parents in how to spot and talk to their children about inappropriate online relationships.

Staff Training: All staff receive training to help them:

- Understand the continuum from HSB to sexual violence
- Recognise the signs of harmful sexual behaviour
- Respond appropriately to disclosures or concerns
- Understand the difference between typical sexual development and concerning behaviour

12.6 Online Learning

Keeping pupils and teachers safe during remote learning is essential; if children are asked to learn online at home specific guidance will be provided to parents and, age appropriately, to children. Teachers delivering remote education online should be aware that the same principles set out in the school code of conduct will apply; specifically:

- Online “Zoom” meetings for the school community are password protected
- Group meetings will have at least two members of staff online at all times

- Environment and clothing checks are an essential part of pre-zoom class preparation.

The Department of Education has produced advice to support safe online learning for teachers, pupils and parents: safeguarding-and-remote-education

12.7 Modern Slavery and Financial Exploitation

Cobham Montessori School recognises that children can be vulnerable to modern slavery and financial exploitation through online means.

Modern Slavery: Modern slavery encompasses human trafficking, forced labour, and domestic servitude. Children may be groomed or coerced online into situations of modern slavery, including:

- Being recruited for criminal exploitation (such as county lines drug trafficking)
- Being trafficked for sexual exploitation
- Being forced into labour or servitude

Financial Exploitation: Children may also be targeted for financial exploitation online, including:

- Being coerced into sharing bank details or financial information
- Being manipulated into fraudulent activities
- Being exploited through online gambling or gaming
- Being pressured into making purchases or transferring money
- Being recruited into money laundering activities (money muling)

Our Response:

- Staff are trained to recognise signs that a child may be at risk of modern slavery or financial exploitation
- Our E-Safety and PSHE curriculum includes age-appropriate education about these risks
- Our filtering and monitoring systems help identify concerning online activity
- All concerns are managed in accordance with our Safeguarding and Child Protection Policy
- We work with external agencies, including the police and children's social care, where appropriate

12.8 Supporting Vulnerable Groups Online

Cobham Montessori School recognises that certain groups of children may face additional vulnerabilities when using technology and the internet.

Young Carers: We recognise that young carers may:

- Use the internet to seek information and support about caring responsibilities
- Be at risk of sharing personal or sensitive information online
- Face barriers to accessing online safety education due to caring responsibilities
- Benefit from online communities and support networks

Children with Medical Conditions: We recognise that children with specific medical conditions may:

- Use technology to manage their health (such as medical devices or apps)
- Require additional support to access online learning
- Be vulnerable to online exploitation related to their condition
- Benefit from online support communities

Our Response:

- We consider the specific needs and vulnerabilities of these groups when delivering E-Safety education
- We provide individualised support where needed
- We ensure that reasonable adjustments are made to enable all children to access online safety education
- We work with parents and carers to understand each child's specific needs and circumstances

13.0 Community Use of the Internet

Staff/Volunteers Use of IT Systems:

Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read the 'Code of Conduct for Staff before using any school ICT resource.

In addition:

- All staff will receive annual update for E-Safety training.
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password protected computers and other devices.
- In lessons where Internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit. They should ensure that at all times the filtering softwares are in use, as well as those that generate reports of websites visited through the school day. These systems should be checked at least once a term, to ensure they are live and in operation.
- Occasionally students may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites from the filtered list for the period of study. Every request to do so should be auditable, with clear reasons for the need.
- Members of the community and other organisations using the school internet connection will have read the guest AUP so it is expected that their use will be in accordance with the school E-Safety policy.

14.0 Communication of the Policy

To pupils

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the AUP as part of their E-Safety education.

To staff

- All staff are shown where to access the e-safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff receive E-Safety training as part of their safeguarding training.

To parents

- The school asks all new parents (as applicable) and pupils (as applicable) to sign the parent/pupil agreement following their child's starting date at the school and before the child is granted access to IT systems.

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters and on the school web site.
- Parents are reminded of e-safety issues through our newsletter.

Cobham Montessori School recognises the crucial role that parents play in the protection of their children with regards to online safety. From time to time the school organises an awareness session for parents with regards to E-Safety which looks at emerging technologies and the latest ways to safeguard children from inappropriate content. The school will also provide parents and carers with information through newsletters, web site and parent meetings.

Parents and carers are always welcome to discuss their concerns on E-Safety with the school, who can direct them to the support of our E-Safety officer if required. Parents and carers will be encouraged to support the school in promoting good E-Safety practice.

This Policy which is applicable to the whole school is part of our Safeguarding Policy and Procedures

Appendix 1: Online Safety – Areas of Risk

We recognise that any users of the internet may be harmed by:

Content (what they may see):

- Exposure to inappropriate videos. pictures or messages which might upset, worry or frighten them
- Imitating harmful or inappropriate behaviour they see online
- Searching for inappropriate content on purpose or stumbling upon it by accident. This would include using voice activated tools to search for content
- Inadvertently giving apps or websites permission to share their location or other personal information
- Exposure to AI-generated content that is inappropriate, inaccurate, biased, or harmful, including deepfakes

Contact (who might communicate with them):

- Being abused online (including sexually) by people they don't know, such as when gaming or using video chat
- Being abused online (including sexually) by people they know, such as friends and family members
- Sending images or information to people on the device's contact list

Conduct (how they might behave):

- Exhibiting unhealthy behaviours and boundaries around their use of screens.
- Being unkind to each other online as well as offline; this could be using mean words or by excluding others from their games.
- Using words or terminology which are not appropriate for their age.
- Engaging in unhealthy relationships.
- As part of natural development, early years children may exhibit curiosity about their own and others' private body parts; if this occurs via technology children may be at risk of taking inappropriate or indecent images and videos of themselves – the Brook traffic light tool can help practitioners to determine whether sexual behaviour is normal healthy sexual development or harmful behaviour which is a cause for concern.

Commerce (financial consequences):

- Risks such as online gambling
- Unintentional in-app purchases - spending real money via in-app or in-game purchases
- Inappropriate advertising
- Phishing and/or financial scams. If children or members of staff report any issues, we will report it to the Anti-Phishing Working Group (https://apwg.org/).
- Financial exploitation, including being coerced into sharing financial information or participating in fraudulent activities
- Modern slavery, including being recruited or coerced into criminal exploitation online

Procedures to Keep Children Safe:

- Check apps, websites and search results before using them with children.
- Children in the Children's House should always be supervised closely when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.
- Make use of home visits and discussions with parents to inform your understanding of how technology is used within the home and the context of the child with regards to technology.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately.
- Read books such as 'The Internet is a Puddle'; 'Smartie the Penguin' and 'Digiduck' or to help children understand the potential dangers of using the internet without guidance from a trusted adult.

https://www.thinkuknow.co.uk/professionals/resources

Appendix 2: Roles and Responsibilities

Our nominated e-Safety Officer is Shona Dolan who has responsibility for ensuring online safety will be considered an integral part of everyday safeguarding practice. This role overlaps with that of the Designated Safeguarding Lead (DSL) role and they work alongside the DSL in all matters regarding safeguarding and E-safety.

Their role will include ensuring:

- all staff, volunteers and managers receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- clear and rigorous policies and procedures are applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the children in the school. Such policies and procedures are include the personal use of work-related resources.
- monitoring procedures are transparent and updated as agreed in school policies.
- allegations of misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- effective online safeguarding support systems are in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- an appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- a current record of all staff and Students who are granted access to school ICT systems is maintained.

Appendix 3: Reporting of E-Safety Issues and Concerns Including Concerns Regarding Radicalisation

Cobham Montessori School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding E-Safety should be made to the E-Safety officer Shona Dolan, who will review the issue and take the appropriate action. For students, they are taught to raise any concerns to their class teacher who will then pass this on to the e-safety officer. Complaints of a child protection nature must be dealt with in accordance with our child protection procedure.

Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting children from the risk of on-line radicalisation. Cobham Montessori School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. The Prevent Officer understands how to safeguard and promote the welfare of children and knows where and how to refer children and young people for further help as appropriate by making referrals as necessary to Channel.