CHILD PROTECTION AND SAFEGUARDING - ONLINE SAFETY

Policy applies from EYFS to Sixth Form and to all Staff	
Date policy reviewed:	15.09.2024
Date of next review:	01.09.2025 or earlier to reflect any changes in legislation
Version:	09.24 v1
Author and Designated Safeguarding Lead (DSL)	Mr Chris Collins Contact details ccollins@cliftonhigh.co.uk
Deputy Designated Safeguarding Leads (DDSL)	Miss Claudia Mulholland - Early Years Foundation Stage Contact details cmulholland@cliftonhigh.co.uk Mrs Alice Taylor – Infant and Junior School Contact details ataylor1@cliftonhigh.co.uk Ms Ali Taylor - Senior School Contact details ataylor@cliftonhigh.co.uk Miss Natasha Widdison – Senior School Contact details nwiddison@cliftonhigh.o.uk Mrs Lindsay Bailey – Wellbeing and Mental Health Lead Contact details lbailey1@cliftonhigh.co.uk
Designated Members of Council with responsibility for Child Protection and Safeguarding	Mrs Hilary Vaughan Contact details hvaughan@cliftonhigh.co.uk Mrs Jane Morrison Contact details jmorrison@cliftonhigh.co.uk Dr Jessica Jenkins Contact details jjenkins@cliftonhigh.co.uk

Version	Date	Paragraph	Material change	Approval
09.22 v1	01.09.2022	3 - Filtering 3 - Mobile Computing Devices Appendix C	New filtering paragraph added. New paragraph re the use of school devices and filtering inserted. Insertion of a new paragraph re. additional advice and support.	Mr Luke Goodman
09.23 v1	01.09.2023	All 2.1, 2.2 and 2.3 4	Updated to reflect changes to Keeping Children Safe In Education 2023, specifically: Updated online filtering and monitoring responsibilities. Updated Online Safety section.	Mr Chris Collins
09.24 v1	15.09.2024	2.5 and 5.2	Updated to reflect change in policy re. mobile phones.	Mr Chris Collins

Clifton High School is committed to child protection and safeguarding children and young people and expects all staff, visitors, and volunteers to share this commitment.

Related Policies

Acceptable Use of ICT – Pupils
Child Protection and Safeguarding
Child Protection and Safeguarding - Preventing Radicalisation
Behaviour – Senior School/Infant and Junior School
Child-on-Child Abuse
Data Protection
Data Retention
Online Filtering and Monitoring
Pupil Code of Conduct - Senior School/Infant and Junior School
Staff Acceptable Use of ICT Agreement
Staff Code of Conduct
Taking, Storing, and using Photographs or Video - Parents

1. Introduction

At Clifton High School it is understood that Information and Communication Technology (**ICT**) provides a very important part of the pupils' learning experience and that they exist in an online world. It is also understood that due to the ever-changing nature of the online environment, it is not always possible to be specific about new risks, but it is the underlying intention that matters most.

The aim at Clifton High School is to promote the positive use of ICT and ensure that all staff, pupils, parents, and all those working with pupils recognise the risks and potential dangers that may arise from the use of Internet, Digital and Mobile Technologies (**IDMT**s), that they understand how to mitigate these risks and potential dangers and are able to recognise, challenge and respond appropriately to any online safety concerns so that pupils are kept safe.

The term "online safety" is specifically defined for the purposes of this policy as the process of limiting the risks to pupils and staff when using IDMT through a combined approach to the School's policies and procedures, education, and training.

The main areas of risk for our school community are:

Content	• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language). • So called lifestyle content, for example pro-anorexia/self-harm/suicide. • Hate content. • Content validation i.e. how to check authenticity and accuracy of online content.
Contact	• Grooming. • Cyberbullying in all forms.
Commerce	• Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords. • Privacy issues, including disclosure of personal information or publishing of images/video without consent. • copyright (little care or consideration for intellectual property and ownership).
Conduct	• Digital footprint and online reputation. • Health and well-being (amount of time spent online). • Personally produced sexual imagery (sending and receiving of intimate images).

2. Roles and Responsibilities

2.1 Governors and Head of School

- Take overall responsibility for online safety (and in the case of the nominated governor for Online Filtering and Monitoring, to ensure that the filtering and monitoring systems are effective).
- Ensure that staff receive suitable children protection and safeguarding training (including online safety, filtering and monitoring training).
- Ensure that Clifton High School is an environment in which pupils can learn and staff can work safely whilst using Internet Digital and Mobile Technologies (IDMTs).
- Are aware of the procedures to be followed in the event of a serious online safety incident.

2.2 Designated Safeguarding Lead (DSL)

The DSL has overall responsibility for child protection and safeguarding (including online safety and understanding the School's filtering and monitoring systems) and is trained in online safety issues. The DSL must be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data;
- access to illegal and inappropriate materials;
- inappropriate on-line contact with adults and strangers;
- potential or actual incidents of grooming; and
- cyber-bullying (including child-on-child abuse).

2.3 Staff

- Must follow the Clifton High School Acceptable use of ICT Agreement, the Taking, Storing, and using Photographs or Video. Policy and the Staff Code of Conduct.
- Must attend online safety, filtering and monitoring training (which form part of the annual CPD programme) and are aware of online safety issues related to the use of mobile phones, cameras, smart technology, and hand-held devices and that they monitor their use and implement current school policies regarding these devices.
- Must be aware of current online safety issues and guidance e.g., through Continued Professional Development (CPD), Staff Briefings.
- Should embed online safety issues in all aspects of the curriculum and other school activities.
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant). Pupils are taught basic workplace computer etiquette in Computing.
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

- Report any suspected misuse or problem to the Class Teacher, Form Tutor, Head of Year, DSL, DDSL or DSLS, logging any concerns or actions on CPOMS.
- Model safe, responsible and professional behaviours in their own use of technology.
- Ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g., personal email, text, mobile phones, social networking.

2.4 Parents

- Must follow the Clifton High School policy on Taking, Storing, and using Photographs or Video (Parents).
- Are kept informed of any new issues that may affect pupil safety and which may affect the wider school community. This is done through the Clifton High School Parents bulletin and information evenings organised through the school.
- Consult with the School if they have any concerns about their children's use of technology.
- Read, understand, and promote the Pupils' Code of Conduct and Behaviour Policy with, for the purposes of this policy, reference to the rules for safer internet use.

2.5 Pupils

- Must abide by the principles for the safe use of the internet:
  - email and internet access are a privilege and not a right, and are provided to assist pupils with their work and to help them improve their IT skills;
  - pupils are responsible for the content of any email which is sent from their account. Pupils who act inconsiderately or irresponsibly or abuse the system may have its use withdrawn and a more serious consequence imposed; and
  - pupils should be aware that their school electronic communications may be monitored.
- Follow the School's Code of Conduct - Pupils in relation to the use of mobile phones and other personal internet enabled devices at School, and in relation to taking and using images at School.
- Know and understand the School's Anti-Bullying Policy, which includes cyberbullying.
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials.
- Look after each other, and to report any concerns about the misuse of technology, or worrying issues to a member of staff, who will take appropriate action.
- Treat staff and each other online with the same standards of consideration and good manners as they would during face-to-face contact.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both at the School and at home.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- Know that sanctions for the misuse or attempted misuse of the internet, mobile phones and other electronic devices will be imposed.

3. Education and Training

Pupils receive online safety guidance throughout the school curriculum including in Computing lessons, circle time, PSHE, Health & Wellbeing, Life Skills, Google Safeguarding Classroom and assemblies. They are taught to:

- understand acceptable behaviour when using an online environment/email;
- understand why they should not post or share detailed personal information and to know how to ensure they have turned-on privacy settings;
- understand why they must not manipulate (including by using AI) or post pictures or videos of others without their permission;
- know not to download any files without permission and have strategies for dealing with receipt of inappropriate materials;
- be aware that child sexual exploitation can occur using technology;
- be aware of the possible forms of online sexual harassment;
- be aware that radicalisation can occur through social media and the internet; and
- know how to seek help if they experience problems when using the internet and related technologies and how to report any form of online abuse.

Members of Staff are updated regularly on online safety issues (and receiving training on online filtering and monitoring) through professional development and staff meetings and new members of staff are provided with information and guidance as part of the induction process.

Parents are informed and educated of the issues surrounding online safety through sending information home via the weekly parents bulletin and the use of workshops/presentations in parents evenings.

4. Online Safety

4.1 Use of Personal Equipment in School

At times, both staff and pupils may choose to bring their own personal items of electronic equipment into the School. The use of these items is governed by this policy, the Acceptable Use of ICT Agreements, the Behaviour policies, the Pupil Codes of Conduct, Taking, Storing, and using Photographs or Video (Staff) and the Staff Handbook. Anyone choosing to bring in their own property into the School is doing so at their own risk, and the school is not responsible for any loss or damage to this property whilst in school.

Rules regarding the use of mobile phones by pupils at school are set out in section 9 of Pupil Code of Conduct - Seniors and section 9 of Pupil Code of Conduct - Infants and Juniors.

4.2 Keeping the School Network Safe

The IT Manager is responsible for ensuring that the School's ICT infrastructure is secure and is not open to misuse or malicious attack and the IT Manager, the Finance Director and the governor responsible for online safety are responsible for ensuring that the School meets the online safety technical requirements. For more information see the Online Filtering and Monitoring policy.

4.3 Network Security

The School uses software to ensure that appropriate firewalls are in place to protect the School and its users. In addition:

- All users are required to change their password every 12 months using strong password requirements.
- Users have access only to certain limited areas that they are authorised to use.
- No software installation is possible without the approval of the IT Department.

Email antivirus and spam protection

Clifton High School uses an industry grade protection in Microsoft Office 365 with built in malware and spam capabilities that help protect inbound and outbound messages from malicious software and spam. The IT Manager can provide further granular control and customisation through the Exchange Admin Centre.

General Antivirus Protection

Sophos Antivirus protects every desktop PC or laptop in use in the School. This offers a centralised control, install and clean-up facility in case of virus breakout.

4.4 Online Filtering and Monitoring

The Online Filtering and Monitoring policy sets out the School's policy on filtering online content and monitoring users' activity.

4.5 Wi-Fi network

The Wi-Fi network is totally separated from the domain network. It has been configured to use a Virtual Lan network (VLan), which provides internet access for Clifton High School users using their personal login. The same rules apply for Wi-Fi users as well as desktop users and the Internet content filtering offers good protection.

4.6 Taking, Storing and Using Photographs or Video

Photographs and videos are regularly taken for recording pupils participating in activities or celebrating their achievements and are an effective form of recording their progression (especially in EYFS). It is essential, that photographs or video are taken and stored appropriately to safeguard all pupils. Refer to Taking, Storing, and Using Photographs or Video (Staff) and Taking, Storing and using Photographs or Video (Parents). Members of staff are not permitted to use their personal devices for taking photographs/. **EYFS staff members are prohibited from having their personal devices in the classroom.**

4.7 Data Protection

Clifton High School is committed to following the data protection principles, including the integrity and confidentiality of personal data and complies with the data protection legislation. Refer to the Data Protection and Data Retention policies for more information.

4.8 User Accounts and Passwords

All users of the School's ICT systems log in with an individual username to ensure that they only have access to the data which they have a right to access to. All passwords must meet the School's complexity requirements and are forced to be changed every 12 months.

Users must not share their logon details with others or attempt to log on using another user's account.

Before leaving a computer, all users must ensure it is either locked or logged out, ensuring nobody else can access an individual logon. All users are responsible for any activity that takes place under their user account.

5. Specific safeguarding issues

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers Clifton High School to protect and educate pupils, students, staff, and parents in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

5.1 Areas of risk

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;

- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

5.2 Cyberbullying

Cyberbullying can be a form of child-on-child abuse and will not be tolerated. The Anti Bullying Policy describes the preventative measures and the procedures that will be followed when cases of cyberbullying are identified.

Proper supervision and monitoring of pupils and their online activity and a ban on mobile phones in the Infant and Junior School and a "never seen, never heard" mobile phone policy in the Senior School plays an important part in creating a safe ICT environment at the School; but everyone needs to learn how to stay safe online. Pupils are taught of the possible consequences of cyberbullying and what to do if it happens to them.

5.3 Preventing Radicalisation

Children are vulnerable to extremist ideology and radicalisation. This can occur through many different methods including social media and gaming.

As part of the school's responsibilities under the Prevent Duty, the rules employed by the School's online filtering and monitoring systems are designed to limit potential access to content and sites that could pose a risk to pupils regarding extremism and radicalisation. Refer to Preventing Radicalisation policy.

5.4 Online sexual abuse and exploitation

This may be stand/alone or part of a wider pattern of sexual harassment and /or sexual violence. It may include:

- Non-consensual sharing of sexual images and videos;
- Sexualised online bullying;
- Unwanted sexual comments and messages, including, on social media; and
- Sexual exploitation: coercion or threats.

Child Sexual Exploitation (CSE)

CSE is a form of child sexual abuse, which can occur through the use of technology. This is when an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity in exchange for something the victim needs or wants, and/or for the financial advantage or increased status of

the perpetrator or facilitator.

"Sexting"

Consensual and non-consensual **sharing of nude and semi-nude images and/or videos** (also known as Sexting or youth produced sexual imagery) is the exchange of self-generated sexually explicit images, through mobile picture messages or webcams over the Internet. Pupils may also call it cybersex or sending a nude, semi-nude, picture or selfie. Sexting is illegal. By sending an explicit image, a pupil is producing and distributing child abuse images and risks being prosecuted, even if the picture is taken and shared with their permission. It is easy to send a photo or message, but the sender has no control about how it's passed on. When images are stored or shared online, they become public. They can be deleted on social media or may only last a few seconds on apps like Snapchat, but images can still be saved or copied by others. These images may never be completely removed and could be found in the future, for example when applying for jobs or university.

Pupils may think 'sexting' is harmless, but it can leave them vulnerable to:

- blackmail when an offender may threaten to share the pictures with the pupil's family and friends unless the pupil sends money or more images;
- bullying may result when images are shared with their peers or in school;
- unwanted attention when images posted online attract the attention of sex offenders, who know how to search for, collect and modify images; and
- emotional distress resulting from embarrassment and humiliation. If they are very distressed this could lead to suicide or self-harm.

Pupils are informed of the consequences of sexting and the legal implications through PSHE lessons and assemblies.

5.5 Responding to incidents of misuse

It is expected that all members of the school community will be responsible users of ICT, however, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Non-illegal misuse

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential to report it on CPOMS to the Head of Year/Head of the Infant and Junior School Deputy Head, Pastoral and inform the Head of Information Technology or Network manager, as soon as possible, and it will be dealt with through normal behaviour procedures.

Illegal misuse

If a child protection or safeguarding issue arises then the Child Protection and Safeguarding Policy must be followed. If any misuse appears to involve illegal activity the SWGfL flow chart (Appendix A) is consulted and followed. Illegal activity would include:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material; and
- other criminal conduct, activity, or materials.

Cyberbullying

If cyberbullying has taken place the Anti Bullying Policy will be followed. The DSL (or DDSL) is responsible for ensuring staff are kept fully informed about any issues and their resolution.

Record for reviewing devices/internet sites

If members of staff suspect that any misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation. In such event the SWGfL 'Record for Reviewing devices internet sites (responding to incidents of misuse) will be followed (Appendix B). This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a 'clean' designated computer. The School is more likely to encounter incidents that involve inappropriate rather than illegal misuse.

6. Useful Links

Sources of further information

- www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
- www.swgfl.org.uk/staying-safe
- www.childnet.com
- www.Thinkuknow.co.uk
- www.internetmatters.org
- www.nspcc.org.uk/keeping-children-safe/online-safety
- www.ceop.police.uk

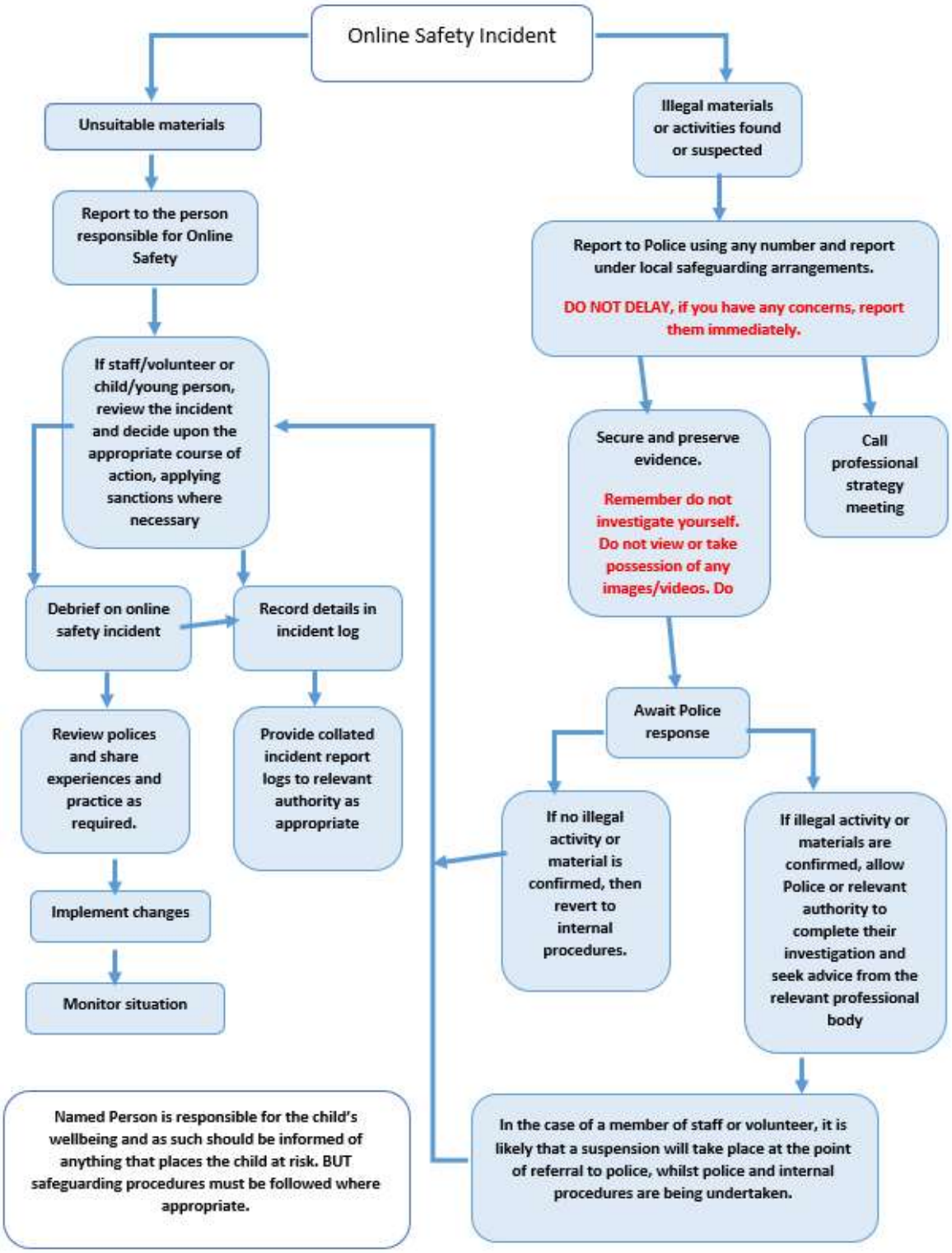
For further links to additional advice and support please see Appendix C.

Clifton High School

Appendix A: SWGfL Flow Chart

The following chart is used for guidance in any e-Safety scenario where illegal activity is suspected.

Clifton High School



Appendix B: Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

Details of first reviewing person

Name: .....
Position: .....
Signature: .....

Details of second reviewing person

Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Clifton High School

Appendix C: Additional advice and support

Online safety-advice

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC E-safety for schools provides advice, templates, and tools on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- Online Safety Audit Tool from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Online safety guidance if you own or manage an online platform DCMS advice
- A business guide for protecting children on your online platform DCMS advice
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Online safety- Remote education, virtual lessons and live streaming

- Case studies for schools to learn from each other
- Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice

- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Online Safety- Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Online safety- Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world
- How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online

- Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment
- #Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships