



**Lift
Hockley**

Online Safety Policy

September 2025

Contents

| | |
|---|----|
| Our commitment | 3 |
| Legislation and guidance | 3 |
| Roles and responsibilities | 4 |
| Educating pupils about online safety | 6 |
| Educating parents about online safety | 7 |
| Cyberbullying | 8 |
| Acceptable use of the internet in the school | 9 |
| Pupils using mobile devices in the school | 9 |
| Staff using work devices outside of the school | 10 |
| How the school will respond to issues of misuse | 10 |
| Training | 10 |
| Monitoring arrangements | 11 |
| Links with other policies | 11 |

.....

Appendix 1: [Online safeguarding issues](#)

Appendix 2: [ICT Acceptable Use Policy](#)

Appendix 3: [Lift Schools student/pupil Online Safety charter](#)

Appendix 4: [Useful links and resources for staff, pupils and parents](#)

Appendix 5: [Delivering online learning safely - 12 tips](#)

1. Our commitment

- 1.1. Lift Hockley is committed to bringing our academies and school support services together to work as with lift schools to ensure safer lives and even more remarkable learning for all children and young people. As we increasingly work, learn and teach online, it is essential that children are safeguarded from potentially harmful and inappropriate online material.
- 1.2. The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. Please see [Appendix 1: Online safeguarding issues](#)
- 1.3. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
 - a) **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
 - b) **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
 - c) **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- 1.4. Accordingly, we have appropriate internet filtering within our school and our central support services and we utilise [eSafe](#) to monitor all activity within our Lift Schools Google suite of applications; in particular the content of information, the nature of the contact and the conduct of the user. The welfare and safety of each individual child is paramount and therefore we are committed to providing a safe online learning environment by:
 - a) Ensuring robust processes are in place to ensure the online safety of pupils, staff, volunteers and governors.
 - b) Delivering an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
 - c) Establishing clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

- 2.1. This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education 2020](#) and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department's Prevent guidance on [protecting children from radicalisation](#).
- 2.2. This policy reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers

stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

- 2.3.** This policy complies with our funding agreement and articles of association.
- 2.4.** We also follow the online safety guidance as recommended within Keeping Children Safe in Education 2020 within our delivery of remote education, virtual lessons and live streaming. This includes a range of resources and guidance for school staff, parents and carers, pupils in Appendix 4: [Useful links and resources for staff, pupils and parents](#)

3. Roles and responsibilities

3.1. The Lift Schools Board of Trustees

The Board of Trustees delegates responsibility for ratifying the online safety policy at each review to the Executive Committee.

3.2. The Headteacher/Principal

The school headteacher/principal is responsible for:

- a) ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- b) ensuring that all staff sign to agree and adhere to the [ICT Acceptable Use Policy](#).
- c) monitoring incident reports produced by eSafe and taking appropriate action if necessary.

3.3. The school Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our [Safeguarding and Child Protection policy](#). The DSL takes lead responsibility for online safety in school, in particular:

- a) Supporting the headteacher/principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- b) Working with the headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
- c) Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- d) Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- e) Updating and delivering staff training on online safety
- f) Liaising with other agencies and/or external services if necessary
- g) Providing regular reports on online safety in school to the headteacher and/or governing board
- h) Monitoring eSafe incident reports, where designated to do so and taking appropriate action.
- i) Ensuring staff involved in the delivery of online learning follow the safety guidance in Appendix 5: [Delivering online learning safely - 12 tips](#)

3.4. The school IT manager/lead

The IT manager/lead is responsible for:

- a) Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. This includes the implementation and maintenance of the [eSafe](#) system.
- b) Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- c) Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- d) Ensuring that any online safety incidents are recorded and dealt with appropriately in line with this policy
- e) Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy

3.5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers will be vigilant to ensure the safe use of online technology and be particularly aware of pupils who may be more vulnerable, e.g. SEND pupils, pupils who are at risk of radicalisation as detailed in section 5 of our [Child protection and Safeguarding policy](#). Staff are responsible for:

- a) Maintaining an understanding of this policy
- b) Implementing this policy consistently
- c) Signing to show their agreement and intention to adhere to the terms on the [ICT Acceptable Use Policy](#) and ensuring that pupils follow the school's terms on acceptable use [Lift Schools student/pupil Online Safety charter](#)
- d) Working with the DSL to ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy
- e) Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy.

3.6. The Trust Designated Safeguarding Lead (DSL)and deputy DSL

The Trust DSL will support school DSLs by:

- a) Providing opportunities to share best practice with each other at virtual, regional and national conferences and with other organisations, e.g. NSPCC, Child Exploitation Online Protection training.
- b) Providing regular updates and resources through the Google+ community and the One Lift Schools safeguarding site. .
- c) Providing support and guidance on specific matters relating to online safety as appropriate.

3.7. Parents

Parents are expected to:

- a) Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- a) What are the issues?, UK Safer Internet Centre:
<https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- b) Hot topics, Childnet International:
<http://www.childnet.com/parents-and-carers/hot-topics>
- c) Parent factsheet, Childnet International:
<http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>
- d) Think U Know - resources and information by the National Crime Agency:
<https://www.thinkuknow.co.uk/>
- e) Resources and information from the NSPCC: [Net Aware](#)

3.8. Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use, see Appendix 2: [ICT Acceptable Use Policy](#).

4. Educating pupils about online safety

4.1. Pupils will be taught about online safety as part of the curriculum. We educate pupils about online safety at an age appropriate level and in accordance with DfE guidance as outlined in: [Teaching pupils about online safety](#)

4.2. In **Key Stage 1**, pupils will be taught to:

- a) Use technology safely and respectfully, keeping personal information private
- b) Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Key Stage 2**, pupils will be taught to:

- a) Use technology safely, respectfully and responsibly
- b) Recognise acceptable and unacceptable behaviour
- c) Identify a range of ways to report concerns about content and contact

4.3. The safe use of social media and the internet will also be covered in other subjects where relevant for example PSHE.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite relevant speakers to present to pupils.

5. Educating parents about online safety

5.1. The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents on our website.

5.2. Online safety will also be covered during parents' evenings.

5.3. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

- 5.4. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyberbullying

6.1. Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victims.

The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes when appropriate, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

See also [Appendix 1: Online safeguarding issues](#) for information relating to other online safeguarding issues.

6.3. Examining electronic devices

school staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- a) Cause harm, and/or
- b) Disrupt teaching, and/or

- c) Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- a) Delete that material, or
- b) Retain it as evidence (of a criminal offence or a breach of school discipline)
- c) Report it to the police

Any searching of pupils must be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in the school

- 7.1. All staff, volunteers and governors annually affirm their agreement regarding the acceptable use of the school's IT systems and the internet through the Code of Conduct. Pupils and parents are expected to confirm their understanding and agreement of their obligations through the [Lift Schools student/pupil Online Safety charter](#)). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.**
- 7.2.** Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- 7.3.** We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in the school

- 8.1.** Pupils may bring mobile devices into the school, but are not permitted to use them.
- 8.2.** Pupils are to turn off and hand-in their mobile devices on arrival to school. The mobile phones are then returned as they leave.
- 8.3.** Any use of personal mobile devices by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.
- 8.4.** When pupils are working within the Lift Schools Google suite of applications on laptops or home computers outside of the school, their activity will still be subject to eSafe monitoring.

9. Staff using work devices outside of the school

- 9.1.** Staff members using a work device outside of the school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in the **Appendix 2: [ICT Acceptable Use Policy](#)**.
- 9.2.** Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of the school. Any USB devices containing data relating to the school must be encrypted.

- 9.3. When staff are working on work devices outside of the school and within the Lift Schools Google suite of applications, their activity will still be subject to eSafe monitoring.

10. How the school will respond to issues of misuse

- 10.1. Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- 10.2. Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- 10.3. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents should be reported to the police.

11. Training

- 11.1. All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- 11.2. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- 11.3. The school DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- 11.4. Local governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- 11.5. Volunteers will receive appropriate training and updates, if applicable.
- 11.6. More information about safeguarding training is set out in our safeguarding and child protection policy [Safeguarding and child protection policy](#)

12. Monitoring arrangements

- 12.1. The DSL (and deputy/deputies)) monitor behaviour and safeguarding issues related to online safety including any monitoring notifications from eSafe.

13. Links with other policies

- 13.1. This online safety policy is linked to the following policies:

| | |
|-------------------------------------|-------------------------------|
| • Safeguarding and child protection | • Mental Health and Wellbeing |
| • Behaviour | • Health and Safety |
| • Staff code of conduct | • Attendance |
| • Acceptable Use Policy | • Recruitment and Selection |

| | |
|--|---|
| <ul style="list-style-type: none"> • Anti-bullying | <ul style="list-style-type: none"> • Data Protection |
| <ul style="list-style-type: none"> • Racist incidents | <ul style="list-style-type: none"> • Curriculum |

Appendix 1: Specific safeguarding issues related to online safety

1. Cyberbullying:

- 1.1. Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)
- 1.2. 1.2 Cyberbullying can also be a form of peer on peer abuse through sexual harassment that happens through the use of technology online. For example, young people may be persuaded or forced to share sexually explicit images of themselves, have sexual conversations by text, or take part in sexual activities using a webcam.

2. Preventing and addressing cyber-bullying

- 2.1. To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- 2.2. The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes when appropriate, and the issue will be addressed in assemblies.
- 2.3. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- 2.4. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- 2.5. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- 2.6. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- 2.7. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

3. Preventing radicalisation

- 3.1. Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk is part of our safeguarding approach.
- 3.2. We are particularly vigilant to any online behaviour that suggests any radicalised behaviour through our eSafe programme.

4. Extremism

- 4.1. Extremism goes beyond terrorism and is defined as the vocal or active opposition to our fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs.
- 4.2. This also includes calling for the death of members of the armed forces (As defined in the Government's Counter Extremism Strategy)
- 4.3. Extremists often target the vulnerable - including the young- by seeking to sow divisions between communities on the basis of race, faith or denomination; justifying discrimination towards women and girls; seeking to persuade others that minorities are inferior; or arguing against the primacy of democracy and the rule of law in our society.

5. Radicalisation

- 5.1. Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- 5.2. There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability.
- 5.3. Similarly, radicalisation can occur through many different methods (such as social media) and settings (such as the internet). However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised.
- 5.4. As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include the designated safeguarding lead (or deputy) making a referral to the Channel programme.

6. The Prevent duty

- 6.1. All schools and colleges are subject to a duty under section 26 of the CounterTerrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism".
- 6.2. This duty is known as the **Prevent** duty. The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders should familiarise themselves with the Revised Prevent duty guidance: for England and Wales, especially paragraphs 57-76 which are specifically concerned with schools (and also covers childcare). The guidance is set out in terms of four general themes: Risk assessment, working in partnership, staff training, and IT policies. Schools have a duty to prevent children from being drawn into terrorism. The DSL will undertake Prevent awareness training and make sure that staff have access to appropriate training to equip them to identify children at risk.
- 6.3. We will assess the risk of children in our school being drawn into terrorism. This assessment will be based on an understanding of the potential risk in our local area, in collaboration with our local safeguarding children board and local police force.
- 6.4. We will ensure that suitable internet filtering is in place (esafe), and equip all pupils to stay safe online at school and at home.
- 6.5. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. Radicalisation can occur quickly or over a long period. Staff will be alert to changes in pupils' behaviour to ensure early identification of risk.
- 6.6. The government website [Educate Against Hate](#) and charity [NSPCC](#) say that signs that a pupil is being radicalised can include:

- 6.6.1. Refusal to engage with, or becoming abusive to, peers who are different from themselves
- 6.6.2. Becoming susceptible to conspiracy theories and feelings of Persecution
- 6.6.3. Changes in friendship groups and appearance
- 6.6.4. Rejecting activities they used to enjoy
- 6.6.5. Converting to a new religion
- 6.6.6. Isolating themselves from family and friends
- 6.6.7. Talking as if from a scripted speech
- 6.6.8. An unwillingness or inability to discuss their views
- 6.6.9. A sudden disrespectful attitude towards others
- 6.6.10. Increased levels of anger
- 6.6.11. Increased secretiveness, especially around internet use
- 6.6.12. Expressions of sympathy for extremist ideologies and groups, or justification of their actions
- 6.6.13. Possessing extremist literature
- 6.6.14. Being in contact with extremist recruiters and joining, or seeking to join, extremist organisations

7. Children who are at risk of radicalisation may have low self-esteem, or be victims of bullying or discrimination.

- 7.1. It is important to note that these signs can also be part of normal teenage behaviour – staff should have confidence in their instincts and seek advice if something feels wrong.
- 7.2. If staff are concerned about a pupil, they will follow our procedures set out in this policy, including discussing their concerns with the DSL. Staff should always take action if they are worried. Further information on the school's measures to prevent radicalisation are set out in other school policies and procedures, including:

8. Additional support

- 8.1. The department has published advice for schools on the Prevent duty. to complement the Prevent guidance and signposts other sources of advice and support. Prevent duty guidance: for further education institutions in England and Wales that applies to colleges. Educate Against Hate, a website launched by Her Majesty's Government has been developed to support and equip school and college leaders, teachers, and parents with information, tools and resources (including on the promotion of fundamental British values) to help recognise and address extremism and radicalisation in young people. The platform provides information on and access to training resources for teachers, staff and school and college leaders, some of which are free such as Prevent e-learning, via the Prevent Training catalogue.

9. Channel

- 9.1. Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation.
- 9.2. An individual's engagement with the programme is entirely voluntary at all stages. Guidance on Channel is available at: Channel guidance, and a Channel awareness e-learning programme is available for staff at: Channel General Awareness.
- 9.3. The school or college's Designated Safeguarding Lead (and any deputies) should be aware of local procedures for making a Channel referral.

- 9.4. As a Channel partner, the school or college may be asked to attend a Channel panel to discuss the individual referred to determine whether they are vulnerable to being drawn into terrorism and consider the appropriate support required.

10. Contextual factors

- 10.1. Safeguarding incidents and/or behaviours can be associated with factors outside the school /or can occur between children outside the school or college. This can involve violent, humiliating and degrading sexual assaults, but does not always involve physical contact and can happen through the use of technology online. For example, young people may be persuaded or forced to share sexually explicit images of themselves, have sexual conversations by text, or take part in sexual activities using a webcam.
- 10.2. All staff, but especially the designated safeguarding lead (or deputy) should be considering the context within which such incidents and/or behaviours occur. This is known as contextual safeguarding, which simply means assessments of children should consider whether wider environmental factors are present in a child's life that are a threat to their safety and/or welfare.
- 10.3. Children's social care assessments should consider such factors so it is important that schools and colleges provide as much information as possible as part of the referral process. This will allow any assessment to consider all the available evidence and the full context of any abuse.

Appendix 4: Useful links and resources for staff, pupils and parents

Opportunities to teach online safety to pupils:

- [Be Internet Legends](#) developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- [Disrespectnobody](#) is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- [Education for a connected world](#) framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- [PSHE association](#) provides guidance to schools on developing their PSHE curriculum
- [Teaching online safety](#) in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- [Thinkuknow](#) is the National Crime Agency/CEOPs education programme with age specific resources
- [Sexting: responding to incidents and safeguarding children](#) - UK Council for Internet Safety. UK Safer Internet Centre has developed further guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Advice for governing bodies/proprietors and senior leaders

- [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](#) provides advice on all aspects of a school or college's online safety arrangements
- [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
- UK Council for Internet Safety have provided advice on [sexting-in-schools-andcolleges](#) and [using-external-visitors-to-support-online-safety-education](#)

Remote education, virtual lessons and live streaming

- [Case studies on remote education practice](#) are available for schools to learn from each other
- [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
- [National cyber security centre](#) guidance on how to set up and use video conferencing
- [UK Safer Internet Centre](#) guidance on safe remote learning

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

Parental support

- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, 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](#)
- [Government advice about security and privacy settings](#), blocking unsuitable content, and parental controls
- [Internet Matters](#) provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [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
- [Lucy Faithfull Foundation StopItNow](#) resource 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
- Parent info from [Parentzone](#) and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- [UK Safer Internet Centre](#) provide tips, advice, guides and other resources to help

