



Grange Primary School

Pursuing excellence for every child

Online Safety Policy

Date Reviewed: March 2025

Next Review: March 2026

Online Safety Policy

This Online Safety Policy outlines the commitment of Grange Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Rationale

Digital technologies have become an integral part of our lives. More time is spent online now than ever before and it is becoming increasingly easier to access for children. In order to keep our children safe, both in our care and outside of school, Grange Primary School understands the importance of Online Safety. ~~We feel~~ It is essential to equip our children with the necessary knowledge and skills to keep themselves safe in the ever growing digital world. Children should have an entitlement to safe access to these digital technologies. The Online Safety Policy is primarily safeguarding and therefore should be viewed alongside other policies including those for Anti Bullying, Safeguarding, Child Protection as well as the Computing and Acceptable Use Policies.

Responsibilities

Online Safety covers a wider scope than just internet use, a summary of the school's Online Safeguarding responsibilities is outlined below. This list will assist in developing a coordinated and effective approach to Online Safety issues

Headteacher & Senior Leadership Team Members

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and deputy head should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring

Designated Safeguarding Lead

- To hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- Work alongside the Online Safety Lead.

Online Safety Lead

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide training and advice for staff/governors/parents/carers/learners
- liaise with (external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce

Governors

- Liaise with the Designated Safeguarding Lead / Online Safety Lead
- receive (collated and anonymised) reports of online safety incidents
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- report to relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

IT Service Provider.

The IT Provider is responsible for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems.*
- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- ensuring the school technical infrastructure is secure and is not open to misuse or malicious attack
- ensuring the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority.
- Ensuring there is clear, safe, and managed control of user access to networks and devices
- Keeping up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Ensuring the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Tom Newling/ Carly Plaskitt for investigation and action
- Ensuring the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Teaching Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use policy.

- they immediately report any suspected misuse or problem to Tom Newling/Harriet Salt for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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 lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

Purpose of this policy

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- To deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

Teaching and learning

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support professional work of staff and to enhance the schools' management functions. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils learn through use of the internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security. Online safety will be embedded into the curriculum whenever ICT is used, staff will ensure that there are positive messages about the safe use of technology and risks as part of their learning as well as planned lessons as part of their Computing curriculum and through Digital Citizenship lessons using the Common Sense Education scheme.

- All staff must read and sign the Staff Acceptable ICT Use Agreement before using any school ICT resource.
- Pupils will read and sign the Pupil Acceptable Use Agreement each year.
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.
- Staff will guide pupils in online activities that support learning outcomes planned for the pupils' age and maturity.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content by reporting it to their teacher or to the Online Safety Lead/ DSL

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know The safe use of social media and the internet will also be covered in other subjects where relevant.

Managing Internet Access

Information system security

- Grange Primary School's computing systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- Pupils must not bring in USBs from home.

E-mail use by pupils

Presently, pupil email is not activated. In the event that email was to be permitted for pupils:

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Pupils must not access others' pupil's accounts or files.
- Incoming emails should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how emails from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

- Staff are reminded that emails are subject to 'Freedom of Information' requests and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted, similarly use of personal email addresses for work purposes is not permitted.
- Pupils must be responsible for their own behaviour on the internet, just as they are anywhere else in the school.
- They will be taught the rules of etiquette for email and will be expected to follow them.
- Access in school to external personal email accounts may be blocked

School Provided Wi-Fi

The whole school building is covered by high speed fibre optic broadband via Wireless Access Points. The purpose of the Wi-Fi is to allow school devices, either used by staff or pupils to access the internet for the purposes of teaching and learning. This is closely monitored by our filtering system.

Personal devices may not be connected to our school Wi-Fi under any circumstances. All incidents where a private device is linked to the system will be picked up and reported by our Filtering System and may lead to further action being taken.

Published content and the school website

Staff or pupil personal contact information will not be published. The contact details given online is that of the school office. The Head teacher and Deputy will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. The school will consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
- Written permission from parents or carers is obtained on admission before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents/carers.
- Parents are clearly informed of the school policy on image taking and publishing on school platforms.
- On Tapestry, only photos of individuals are uploaded to the child's journal, which cannot be accessed by other parents/carers.
- Staff may upload images of children to Padlet but these will not be shared with parents unless permission has been given.

Social networking and personal publishing

- At Grange Primary School we block access to social networking sites and newsgroups unless a specific use is approved. The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils will be advised to use nicknames and avatars when using social networking sites for use at home.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Refer to the Social Media Policy for Grange Primary School.

Managing filtering

If staff or pupils come across unsuitable online materials, the site must be reported to the Computing leader. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school will use Google safe search to enhance our filtering capabilities.

Pupils will be taught through Online Safety lessons safe methods to search the internet and what to do if they come across inappropriate content.

The DSL and Online Safety Officer will monitor the filtering report every two weeks alongside a computer technician from our provider.

Managing video conferencing & webcam use

Videoconferencing should use the educational broadband network to ensure quality of service and security.

When at school, staff should be aware of potential breaches of GDPR and Safeguarding, e.g. ensuring the background is clear of any personal/school information or photographs.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The senior leadership team are aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile Devices.

Pupils will not be permitted to bring mobile phones into school.

Staff must ensure that personal mobile devices are switched to silent and put away during teaching times. In exceptional situations where a staff member needs to take a call for personal reasons, permission must be sought from the Head teacher.

Staff wearing smart watches that connect to personal mobile devices **MUST** be set to 'do not disturb' while in school.

Pupils are not permitted to bring smart watches/devices onto school premises.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing risks

The school 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 or to eliminate risks completely. Neither the school nor NELC can accept liability for any material accessed, or any consequences of internet access. The school will audit Computing use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet filtering

We use Meraki as our filtering service and this is monitored by our IT Support Provider, Education Lincs. The filtering service allows the school to monitor internet use and prevent inappropriate or offensive materials from being accessed.

Staff Email

All staff have use of Gmail, which is provided as part of our Google For Education package.

Email is an effective business tool for communicating with colleagues, parents, suppliers etc. inside and outside the school. Email is not a secure means of communication. It does not provide immediate or guaranteed delivery. All emails sent or received using the school's systems are the property of the school. All messages will be unpacked and scanned for viruses as they arrive or leave all school systems.

Users of school Email shall:

- Send all sensitive information using MOVEIT. This will also indicate to the recipient how you expect them to handle the information
- Ensure emails never contain children's full names either in the subject line or the main body of the text. Initials should be used wherever possible.
- Treat unsolicited Emails from unknown sources with suspicion.

Users of school Email shall not:

- Use language which includes swear words, or be offensive or abusive.
- Send school information to or from your own personal email address especially where this includes sensitive personal information of a pupil or staff member
- Download school information to non-school devices or personally controlled cloud storage.
- Set up automatic forwarding of email rules to external email accounts
- Forward "chain" or joke emails to others
- Use school email addresses and other official contact details for setting up personal social media accounts.
- Seek to gain access to another user's mailbox without either their consent or the written approval of their line manager.

Where you are replying to group email messages, take care to remove personal data from the correspondence chain where appropriate. The onus is on the staff of Grange to protect data in transit.

Device Security

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- All staff and pupils will be unable to access any device without unique username and password. The IT support and Computing Leader will be responsible for ensuring that all staff have these details.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Any breach (ie loss/theft of a device or USB keydrives) is to be brought to the attention of the Headteacher immediately.
- Passwords – must not be shared between staff for any reason.
- Keeping operating systems up to date. – All devices will have anti-virus software which will be updated regularly. IT support technicians will be responsible that this is carried out. **In order to receive regular updates, teachers must completely shut their PCs/Laptops down once a week. If this does not happen, anti-virus software could become out of date.**

Handling Online Safety complaints

- Complaints of internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding and child protection procedures and reported to the DSL
- Pupils and parents will be informed of consequences for pupils misusing the internet.
- Notice and take down policy- should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Communications

- Online Safety SMART rules will be posted in all classrooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- All staff will undergo annual training on Online Safety through termly Newsletters emailed out.
- Online Safety training will be embedded within the Computing scheme of work and the Personal Social and Health Education (PSHCE) curriculum. Commonsense
- **All Staff and Volunteers**
All staff and volunteers will sign as read and understood both the Online Safety policy and Staff Acceptable Use Policy.

Staff are to ensure:

- All digital communications are on a professional level and only carried out using official school systems.
- They monitor the use of digital technologies in lessons
- Any Online safety incident is recorded ~~reported~~ on CPOMS and reported to the DSL.
- Staff will be informed that network and internet traffic can be monitored and traced to the individual user.

- Staff that manage filtering systems or monitor Computing use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engines such as Google Safe Search or Kiddle, when accessing the web with pupils.

Parents/Carers

The school will raise parents' awareness of online safety in newsletters or other communications home, and in information via our website or Tapestry. This policy will also be shared with parents. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with class teachers or the Online Safety Lead. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Parents must understand that the school needs to have rules in place to ensure that their child can be properly safeguarded. The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Links with other policies

This online safety policy is linked to our:

Social Media Policy • Child protection and safeguarding policy • Behaviour policy • Staff disciplinary procedures • Data protection policy and privacy notices • Complaints procedure • Computing Policy and the acceptable use agreements.

Date ratified by the Governing Body:

March 2025

Date Last Reviewed

Feb 2025

Next review date:

March 2026

Virtually Signed (Chair of Governors):

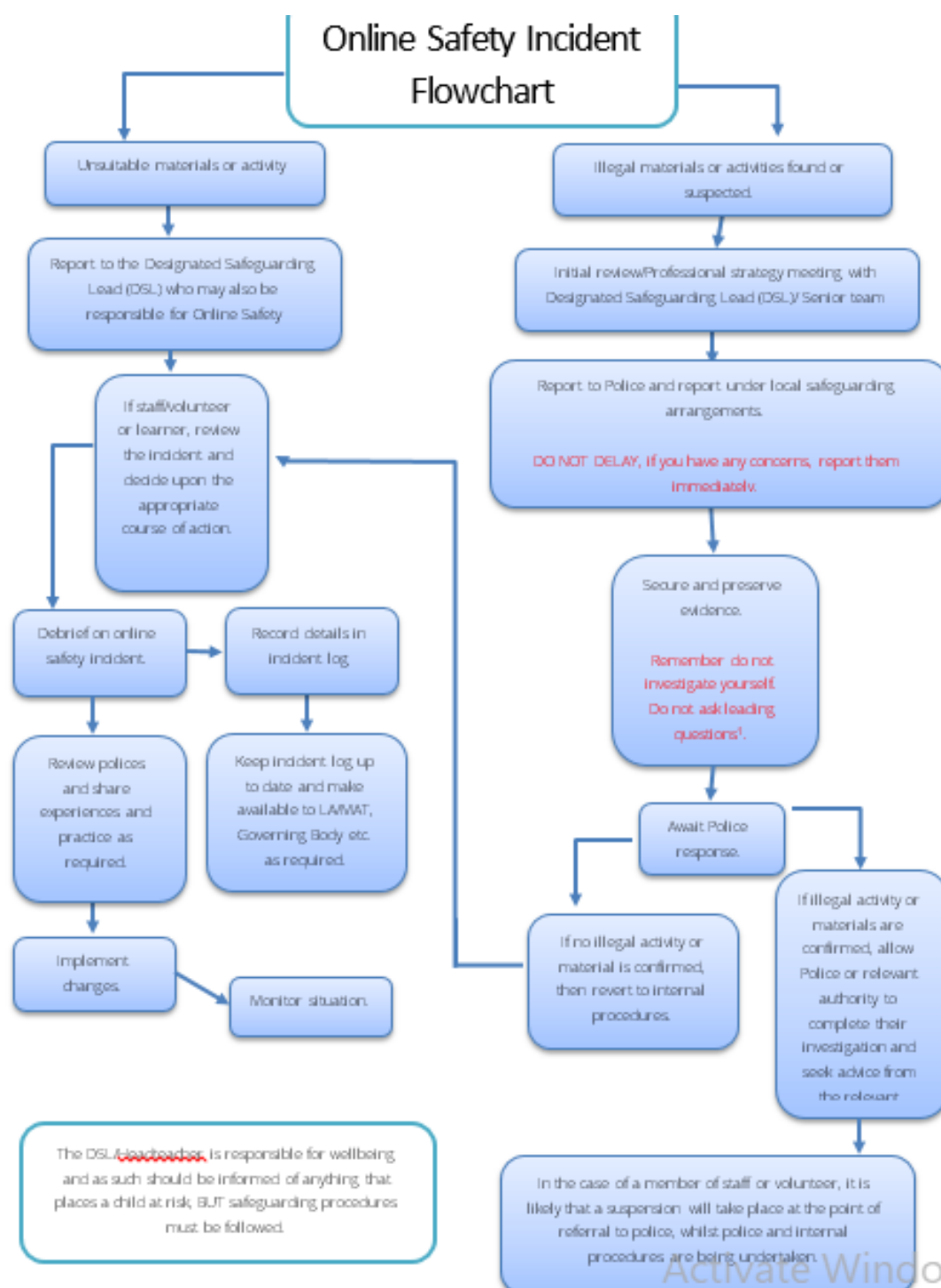
Mr S Ryley

Date: March 2025

Schedule for development, monitoring and review.

This Online Safety Policy was approved by the <i>school governing body</i> on: <i>March 2024</i>	<i>Insert date</i>
The implementation of this Online Safety Policy will be monitored by:	<i>Insert name of individual/group (e.g. designated safeguarding lead, online safety lead, senior leadership team, other relevant person/group)</i>
Monitoring will take place at regular intervals:	<i>Once a year</i>
The <i>governing body</i> will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>Insert time period (suggested to be at least once a year)</i>

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>Insert date</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>Insert names/titles of relevant persons/agencies, e.g. MAT officers, LA safeguarding officer, police etc</i>



Appendix 2: Useful resources for teachers

Websites

WEBSITES

- Common Sense Education

- BBC Stay Safe

www.bbc.co.uk/cbbc/help/safesurfing/

- Becta

<http://schools.becta.org.uk/index.php?section=is>

- Chat Danger

www.chatdanger.com/

- Child Exploitation and Online Protection Centre

www.ceop.gov.uk/

- Childnet

www.childnet-int.org/

- Cyber Café

http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

- Digizen

www.digizen.org/

- Kiddle (Safe search engine for kids)

<http://www.kiddle.co/>

- Kidsmart

www.kidsmart.org.uk/

- Think U Know

www.thinkuknow.co.uk/

- Safer Children in the Digital World

www.dfes.gov.uk/byronreview/

- Be Internet Legends

https://beinternetlegends.withgoogle.com/en_uk

- Education for a Connected World.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf