REDDAM
HOUSE
BERKSHIRE

E-Safety Policy

Reddam House Berkshire is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, students and visitors to share this commitment. This is a whole school policy.

All outcomes generated by this document must take account of and contribute to safeguarding and promoting the welfare of children and young people at Reddam House Berkshire.

Version 6 – September 2023 (LCT)
Review date: August 2024

Contents

Introduction

It is the duty of Reddam House Berkshire to ensure that every student in its care is safe, and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose more significant and subtle risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks.

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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music/video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;

- Online communities via games consoles; and
- Mobile internet devices such as smartphones and tablets.

This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

While exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Reddam House Berkshire we understand the responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. Staff are bound by the school's Code of Conduct which includes acceptable use of the school's IT systems and equipment. 'Parents includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Agreements cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.) as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smartphones, etc.).

Education and Training

Staff: awareness and training

New teaching staff receive information on Reddam House Berkshire's e-Safety and Acceptable Use Agreements as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time and are made aware of their responsibilities relating to the safeguarding of children within the context of e-safety, including filtering and monitoring. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Agreement, which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A CPOMS incident must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's DSL. The School’s DSL keeps a log of any reported incidents on CPOMS.

Students: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to students on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our students' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and computing IT lessons. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via our Aspire to Be (A2B) programme, or Life Skills in the Junior School, by presentations in assemblies, as well as informally when opportunities arise for all year groups from Reception to Year 13. Visiting speakers may also present on this topic.

At age-appropriate levels, and regularly (via PSHCE lessons, computing, form times, assemblies and other opportunities), students are taught about their e-safety responsibilities and how to look after their online safety. We know our students have access to the internet from an incredibly young age and are also some of the most vulnerable members (because of their age) in our community.

From Reception, students are taught about recognising things such as online sexual exploitation, stalking and grooming, the risks, and importance of reporting any such instances they or their peers come across. Students are aware of things to look out for (posters are displayed around the school) and know who the safeguarding lead in the Junior School is (Marion Mason DDSL). They also know that they can talk to any of their teachers, who will support them by taking the correct actions. Actions arising will be in accordance with the school’s Child Protection/Safeguarding Policy (September 2023).
In addition, all classes have Worry Boxes in their classroom, which they can add things to anonymously or otherwise, and in addition to this, Year 5&6 also have access to Whisper.
Talks, from both Reddam staff and outside sources, are organised regularly to ensure that the importance of online safety is something constantly in students' thoughts and the local PCSO is

also invited to present to Year 5&6 students, as they learn about relevant laws applicable to using the internet; such as data protection and intellectual property.
All students are taught about respecting other people's information and images through discussion and classroom activities.
In the Junior School an off-timetable Internet Safety Day was launched in 2021 and is expected to run bi-annually on Internet Safety Day.

Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Counter-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Students should approach the Designated Safeguarding Lead as well as parents, peers and other school staff for advice or help if they experience these issues when using the internet and related technologies.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about students' behaviour in this area and likewise, it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school therefore arranges biannual discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. The last session was held on September 2023; the accompanying documentation is available on request.

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. When projecting anything onto the screen during a class, it is important to ensure that sensitive information, such as emails or personal documents, are not visible to students. Staff should take extra care to avoid displaying any content that could compromise their privacy or the privacy of their colleagues, by double checking what they are presenting before it appears on the screen.

Staff are referred to the Staff Code of Conduct 2023 for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Reddam House Berkshire are permitted to bring in personal devices for their use. They may use such devices during break-times and lunchtimes and when not teaching/in the presence of students in office areas/staff room.

Staff working in the ELS should note that personal devices MUST be left in the School Office or the staffroom, they are not permitted to be used anywhere in the Early Learning School outside of the school office or staff room.

Non-work telephone numbers, email addresses, or other contact details may not be shared with students or parents/carers and under no circumstances may staff contact a student or parent/carer using a personal telephone number, email address, social media, or other messaging systems.

Students

If students in Years 7-11 bring in mobile devices (e.g. for use during the journey to and from school), they should be kept switched off and out of sight all day (8am-5.15pm), following the Mobile Device and Social Media Policy and will remain the responsibility of the child in case of loss or damage. This is particularly important as many children now have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, could sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.

In the exceptional cases of Year 6 students bringing in a Mobile Device, these must be handed in to the Junior Admin office or form tutor at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology. Mobile devices should only ever be used by a Junior School student on school premises, with permission.

The school has introduced the use of student-owned devices as a teaching and learning tool, and students are required to ensure that their use of tablets for schoolwork complies with this policy and the Student Acceptable Use Policy and prohibits students from using devices for non-school related activities during classes.

The school recognises that mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to use a mobile device for such purposes, the student's parents or carers should arrange a meeting with the Head of School to agree how the school can appropriately support such use. The student's teachers and other relevant members of staff will be informed about how the student will use the device at school.

Use of Internet and Email

Staff

Staff must not access social networking sites, personal email or any website or personal email which is unconnected with schoolwork or business from school devices or while teaching / in front of students. Such access may only be made from staff members' own devices while in staff-only areas of the school. Please see Staff Code of Conduct (September 2023)

When accessed from staff members' devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications and web browsing through the school network and staff email addresses are monitored.

Staff must immediately report to the DSL/ IT Manager, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to the DSL/ IT Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Reddam House Berkshire into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school students or parents be added to social network 'friends' or contacted through social media. (See separate section on ‘Staff who are parents’ in Staff Code of Conduct 2023).

Any digital communication between staff and students or parents/carers must be professional in tone and content. Under no circumstances may staff contact a student or parent/carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Emails to students/parents are conducted through the ISAMS system (Connect system in the ELS) to ensure that all communication is logged in the Communication Log, unless this is of a confidential safeguarding nature..

Students

All students are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure and must be used for all schoolwork. Students should be aware that email communications through the school network and school email addresses are monitored.

There are strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, students should contact the IT team for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the DSL, IT Manager or another member of staff.

The school expects students to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others. Students should also take care to follow the terms of service for any site on which they post.

Students must report any accidental access to materials of a violent or sexual nature directly to the DSL, IT Manager or another member of staff. Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on CPOMS and will be dealt with under the school's Behaviour and Counter-Bullying Policies. Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system (Fortinet) If the filtering system causes problems for schoolwork/research purposes, students should contact the IT team for assistance.

The DSL team receive filtering and monitoring reports (FortiAnalyzer report) each morning at 8am (Daily Cyber-bullying indicators report and Daily Self-harm and risk indicators report). Year co-ordinators will respond to any reports of concern as alerted by the DDSL team. Staff should be constantly checking students screens in lessons and alert to what students are searching in lessons. Any inappropriate usage should be reported immediately to the DSL team.

Course of action if inappropriate content is found

Please also see Behaviour, Rewards and Sanctions Policy and Student Code of Conduct

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
  - Turn off the monitor or minimise the window.
  - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
  - Ensure the well-being of the student.
  - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the students).
  - Report the details of the incident to the DSL.
- The DSL will then:
  - Log the incident and take any appropriate action depending on whether it was deliberate or not.
  - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

E-safety in the boarding house

Parents of boarding students must declare all devices (laptops, phones, tablets) that their child will be bringing into the boarding house, so that they can be collected every evening at bedtime (Yr7-11). Technology collection takes place every evening at times linked to the age or the students. If a student is found to have undeclared technology then this will be confiscated until the end of term and parents and guardians will be made aware of this.

Students may use the school Wi-Fi and any usage during ‘sleeping times’ can be monitored by staff. All social media sites are blocked during school hours and between the hours of 6:30pm and 8:15pm (study time).

If an inappropriate search is reported or discovered to have taken place, students’ technology can be confiscated for a period of 24 hours with parents / guardians being informed and the student will receive sanctions in line with the Behaviour, Rewards and Sanctions Policy, Counter Bulling policy or Safeguarding and Child Protection Policy, depending on the nature of the search that has taken place. Support is also offered to boarders who may need it following any inappropriate searches.

Data storage and processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Privacy Notice, Data Protection Policy and the Acceptable Use Policy for further details.

Staff and students are expected to save all data relating to their work to their Surface Pro/Macbook or the school's central server / One Drive Account.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required to fulfil their role. No personal data of staff or students should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager.

Password security

Students and staff have individual school network logins, email addresses and storage folders on the server. Staff and students are regularly reminded of the need for password security.

All students and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed when automatically instructed on the system
- not write passwords down; and
- not share passwords with other students or staff. Sharing of passwords with students, including passwords to wifi that is not ‘student wifi’ is a breach of the acceptable use policy, staff code of conduct and a safeguarding concern.

Staff should refer to the Inspired policy on Passwords and Account Security.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their images on the internet (e.g. on social networking sites).

Parents/carers are welcome to take videos and digital images of their children at school events for their personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites etc. without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other students in the digital/video images.

Staff can take digital/video images to support educational aims but must follow this policy and the Acceptable Use Policy, Child protection and Safeguarding Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute or to cause embarrassment.

Students must **never** take, use, share, publish or distribute images of others unless express consent has been given. Breaching this will be treated extremely seriously in line with our Mobile Phone and Social Media policy, Counter-Bullying Policy and Behaviour, Rewards and Sanctions Policy. This includes photos taken outside of school but distributed to students within the school without the ***express consent*** of the subject. Please note, for the purposes of sanctions, without proof of express consent it will be assumed that none was given. Any doctoring or images or addition of text which causes embarrassment will be dealt with severely.

Permission from parents or carers (or students in the case of older students) will be obtained before photographs of students are published on the school website or social media sites (see Taking, Storing and Using Images of Children Policy for more information).

Photographs published on the school website, or displayed elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs without the express permission of the parents.

Misuse

Reddam House Berkshire will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and Wokingham Children’s Services (Please see Child Protection and Safeguarding Policy). This includes, but is not limited to, involvement in cyberbullying, consensual and non-consensual sharing of nude and semi-nude images and/or videos, involvement in radicalisation, grooming and other high-risk activities.

Incidents of misuse or suspected misuse must be dealt with by staff following the school's policies and procedures detailed in the Child Protection and Safeguarding Policy.

The school will impose a range of sanctions on any student who misuses technology to undertake inappropriate searches and/or bully, harass or abuse another student in line with our Behaviour, Rewards and Sanctions and Counter-Bullying Policies.

Electronic devices - search and deletion

Schools now have the power to search students for items ‘banned under the school rules' and the power to ‘delete data' stored on seized electronic devices. Summary of the power to search as detailed in the Education Act 2011 can be found here. Only the Principal, Heads of School or other staff member directly authorised by them (e.g. the safeguarding team) may undertake a search for items. An excerpt of the Searching Procedure is copied below.

Dealing with electronic devices

Where the authorised person conducting the search finds an electronic device that is prohibited by the school rules or that they reasonably suspects has been or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so.

They may also delete data or files if they think there is a good reason to do so unless they are going to give the device to the police. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone if it has been seized in a lawful 'without consent' search and is prohibited by the school rules or is reasonably suspected of being, or is likely to be, used to commit an offence or cause personal injury or damage to property.

The authorised member of staff must have regard to the following guidance issued by the Secretary of State when determining what is a "good reason" for examining or erasing the contents of an electronic device:

In determining a 'good reason' to examine or erase the data or files, the staff member should reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

If an electronic device that is prohibited by the school rules has been seized and the member of staff has reasonable grounds to suspect that it contains evidence about an offence, they must give the device to the police as soon as it is reasonably practicable. Material on the device that is suspected to be evidence relevant to an offence, or that is a pornographic image of a child or an extreme pornographic image, should not be deleted before giving the device to the police. Staff should not view images considered to be nudes/semi-nudes.

If a staff member does not find any material that they suspect is evidence in relation to an offence and decides not to give the device to the police, in consultation with the Principal he or she can decide whether it is appropriate to delete any files or data from the device or to retain the device as evidence of a breach of school discipline.

All school staff should be aware that behaviours linked to consensual and non-consensual sharing of nude and semi-nude images put a child in danger. If a staff member suspects a child has been involved in a 'consensual and non-consensual sharing of nude and semi-nude images ' incident this must be **reported immediately to the DSL in accordance with the school's Child Protection/Safeguarding Policy (September 2023)**.

Any data or files which indicates that child-on-child sexual violence and sexual harassment should be **reported immediately to the DSL**. Staff are reminded, in accordance with our Child Protection and Safeguarding Policy that this is not acceptable and will not be tolerated. It should never be passed off as 'banter', 'part of growing up' or 'having a laugh'.

All school staff should be aware that behaviours linked to consensual and non-consensual sharing of nude and semi-nude images put a child in danger, the school's approach to this is reflected in the Child Protection Policy. The UK Council for Child Internet Safety (UKCCIS) Education Group has published the advice - Sharing Nudes and Semi-Nudes - responding to incidents and safeguarding young people

Loading/installing software

For this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free of viruses.
- Only authorised persons, such as the ICT Technician or Computing Subject Leader, may load software onto the school system or individual computers.
- Where staff are authorised to download software to their laptops/devices, they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

Backup and disaster recovery

The school will define and implement a backup regime which will enable recovery of critical systems and data within a reasonable timeframe should a data loss occur. This regime includes:

- The use of a remote location for backup of crucial school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.
- Staff are responsible for backing up their data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server such as the Office 365 Account.
- Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

The school’s ICT disaster recovery plan takes effect when a severe disturbance to the school’s ICT infrastructure takes place, to enable critical school systems to be quickly reinstated and prioritised. The IT Manager takes control of this situation to recover vital data as a priority.

School and the Data Protection Act

Schools must have appropriate security to prevent the personal data held (e.g. for staff, students and parents) being accidentally or deliberately compromised.

The implications of this for the school will be the need to:

- Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach.
- Be clear about who is responsible for ensuring information security.
- Ensure that the school has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.

- Respond to any breach of security swiftly and effectively.

Failure to comply with the Act could result in loss of reputation or even legal proceedings.

Further guidance may be found at www.ico.gov.uk and in the school's Data Protection Policy and Privacy Notices.

Complaints relating to all aspects of E-Safety

As with all issues of safety at Reddam House Berkshire, if a member of staff, a student or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Head of School in the first instance, who will liaise with the Principal and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using CPOMS (see Child Protection and Safeguarding Policy) and reported to the school's Designated Safeguarding Lead following the school's Safeguarding Policies.

Reviewing online safety

Technology, and risks and harms related to it evolve and changes rapidly. Reddam House carries out an annual review of our approach to online safety using the 360 safe website. UKCIS has published Online safety in schools and colleges: Questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping children safe online and how to improve this approach. The safeguarding governor, DSL, SLT and IT technician will review online safety and filtering & monitoring at least annually and following any issues that arise.

Appendix – References and Sources

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. KCSIE has a comprehensive list in Annex D.

https://www.getsafeonline.org/

Childnet International

- The "for working with young people" area contains information for teachers on making the internet a valuable part of the school curriculum, such as articles on hot topics (cyberbullying, social networking, consensual and non-consensual sharing of nude and semi-nude images etc.), lesson plans and advice on reporting concerns.
- The "for you as a professional" area includes a "professional reputation checklist" for personal use of social networks and a "using technology checklist", which covers issues such as school policies, guidelines for contacting students, using personal and work devices, and how to set Internet-related homework.

- The website also includes a lot of information relating to the detection and prevention of cyberbullying.

UK Safer Internet Centre - a partner of Childnet International, South West Grid for Learning and the Internet Watch Foundation: co-funded by the European Commission's "Safer Internet Programme."

The South West Grid for Learning - one of the three charity partners of the UK Safer Internet Centre

Child Exploitation and Online Protection Centre - a National Crime Agency command dealing with criminal/safeguarding concerns and reporting

- *Thinkuknow programme*
  CEOP's Thinkuknow programme provides a range of free educational resources - films, lesson plans, presentations, practitioner guidance, games and posters - to professionals working with children. You can access the resources by registration on the Thinkuknow website or by attending CEOP training.
- *ClickCEOP app*
  CEOP has worked with social networking sites such as Facebook to make internet safety advice easily accessible to children via the ClickCEOP app.
- *CEOP report*
  If you think that someone has acted inappropriately towards a child online, you can make an online CEOP report.

NSPCC's Child abuse and neglect guidance

Education and Training
This website contains specific advice for schools on a range of relevant topics, including Acceptable Use Policies; raising awareness of e-safety issues; e-safety and Ofsted inspections; data safety and security; safety training for staff and helpers; online conduct by staff and helpers; logging and monitoring e-safety incidents; and the role of the e-safety coordinator.

Digizen.org
This website contains useful information about social networking in schools, and how staff can incorporate it into their teaching. There is a "Teachers" link which filters the website to show the most relevant resources, including ideas and activities, practical help, and expert comment.

The UK Safer Internet Centre

The UK Safer Internet Centre provides a wide range of resources for schools, such as:

- **Facebook Checklist** with practical information around privacy settings etc
- **Teachers and Professionals section**, including resources on teaching internet safety, professional reputation, and safety features on social networks; and
- **Professionals Online Safety Helpline** for professionals who work with children and young people in the UK (helpline@saferinternet.org.uk or 0844 381 4772).

360 degree safe
This contains a self-review tool, enabling schools to review their ICT policies, as well as resource links and some template policies.

The UK Council for Child Internet Safety
The UK Council for Child Internet Safety was set up in 2008 and brings together over 200 organisations from government, industry, law, academia and charity sectors to work together to keep children safe online. The Council has published a variety of guidance, including a Code of Practice on Parental Controls. There is no guidance tailored explicitly to teachers.

Filtering and Monitoring

Useful links and resources

Department for Education
Keeping Children Safe In Education (DfE)
Meeting digital and technology standards in schools and colleges (DfE)
Broadband internet standards for schools and colleges (DfE)
Cyber security standards for schools and colleges (DfE)
Data protection policies and procedures (DfE)

Home Office
The Prevent duty: safeguarding learners vulnerable to radicalisation (Home Office)

Information Commissioner's Office
Data Protection Impact Assessment (DPIA) (ICO)

London Grid for Learning (LGfL)
Online Safety Audit (LGfL)

South West Grid for Learning (SWGfL)
Online Safety Review (360Safe) (SWGfL)

National Cyber Security Centre
Cyber security training for school staff

UK Safer Internet Centre
2023 Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)
Test Your Internet Filter (UKSIC / SWGfL)
Filtering provider responses - self-certified by service providers (UKSIC)
A Guide for education settings and filtering providers (UKCIS)
Establishing appropriate levels of filtering (UKSIC)
Online safety in schools and colleges: questions from the governing board (UKCIS)

Digital Resilience

HeadStart Online Digital Resilience Tool (HeadStart Kernow)