

Staines Preparatory School



Online Safety Policy

September 2025

Introduction

The Online Safety Policy relates to other policies including those for Computing, Anti Bullying, Child Protection and Safeguarding, Staff Code of Conduct, Mobile Phone Devices Policy and Computing Acceptable Use.

The school's Online Safety coordinator is the Designated Safeguarding Lead.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

[Teaching online safety in schools](#)

[Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)

[Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It 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.

The policy also considers the National Curriculum computing programmes of study.

Roles and responsibilities

The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness.

The Governing body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

If applicable, add: The governor who oversees online safety is David Brown.

All governors will:

Ensure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) [and deputies] are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

Working with the ICT manager to make sure the appropriate systems and processes are in place

Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents

Managing all online safety issues and incidents in line with the school's child protection policy

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the Headteacher and/or governing body

Undertaking annual risk assessments that consider and reflect the risks children face

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT Manager

The ICT manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Conducting a full security check and monitoring the school's ICT systems on a weekly basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use

Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes.

Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Visitors and members of the community

Visitors and members of the community who use the school's ICT 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

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/>).

This Online Safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies, including the use of school-based devices, the internet, email, instant messaging and other social networking technologies and mobile phones and games, to safeguard adults and pupils. It details how the school will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable use or misuse of these technologies by adults or pupils.

The use of the internet as a tool to develop teaching, learning and administration has become an integral part of school and home life. There are always going to be risks with using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst pupils use these technologies. These risks include:

- Being vulnerable to inappropriate contact from strangers;
- Cyber-bullying;
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices;
- Issues with spam and other inappropriate email;
- Online content which is abusive, offensive, or pornographic;
- The use of social media to encourage extremism; and
- Viruses.

It is also important that staff are clear about the procedures, for example only contacting pupils about homework via the school's learning journal (SeeSaw), not via personal emails.

Whilst we endeavour to safeguard and mitigate against all risks, we will never be able to completely eliminate them all. Any incidents that may come to our notice will be dealt with quickly and according to the school's policies to ensure the school continues to protect pupils.

It is the duty of the school to ensure that pupils, teachers, administrative staff and visitors are protected from potential harm whilst they are on school premises.

The involvement of pupils and parents is also vital to the successful use of digital technologies. This policy thus also aims to inform how parents and pupils are part of the procedures and how pupils are educated to be safe and responsible users so that they can make good judgments about information they see, find and use.

Aims of this Policy

- To ensure the safeguarding of all pupils within the school by detailing appropriate and acceptable use of all online and digital technologies.
- To outline the roles and responsibilities of all pupils, staff and parents.
- To ensure all pupils, staff and parents are clear about procedures for misuse of any online technologies.
- To develop links with parents and the wider community to ensure continued awareness of online technologies.

Pupils

Our pupils:

- Are responsible for following the Acceptable Use Policy whilst within school as agreed each academic year or whenever a new pupil starts at the school for the first time. The rules (Annex 2) are shared with the pupils in the Autumn Term and referred to throughout the year;
- Are taught to use the internet in a safe and responsible manner through, for example, ICT and PSHEE lessons;
- Are taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know;
- Are made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues;
- Are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites;
- Are taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for schoolwork, and be copyright free;
- Are taught to understand what is meant by e-safety through age-appropriate delivery;
- Are taught that sending malicious or hurtful messages outside of the school can become a matter whereby the school may set sanctions or involve outside agencies such as the police;
- Are taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk;
- Are given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by this policy; and
- Must connect to the internet whilst on premises owned by Staines Preparatory School using the pupil wireless network and must not circumvent internet access by using a personal device's cellular data services.

Inappropriate Use by Pupils

Should a pupil be found to deliberately misuse digital or online facilities whilst at school, appropriate sanctions will be applied. If a pupil accidentally accesses inappropriate materials, the pupil is expected to report this to an appropriate member of staff immediately and take action to minimise the screen or close the window. Deliberate abuse or damage of school equipment will result in parents being billed for the replacement costs of the equipment. Should a pupil use the internet whilst not on the school premises in such a way as to cause hurt or harm to a member of the school community, the school will act quickly and in accordance with our Behaviour Policy.

Refer to Annex 1 for further guidance.

Staff

It is the responsibility of all adults within the school to:

- Adhere to the Staff Behaviour Policy including Computing Acceptable Use Policy;
- Implement the pupil Digital Safety Agreement (see Annex 2, 3 and 4);
- Be up to date with digital knowledge appropriate for different age groups;
- Be vigilant when using technology as part of lessons;
- Model safe and responsible use of technology;
- Provide reminders and guidance to pupils on Digital Safety;
- Ensure that pupils are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner;

- Not leave a computer or other device unattended whilst they are logged on;
- Lock away or safely secure all portable ICT equipment when not in use;
- Protect confidentiality and not disclose information from the network, or pass on security passwords;
- Make sure that any information subject to data protection legislation, , is not stored on unencrypted portable media or transported in an unsecure form;
- Use their discretion when communicating electronically about work-related issues and not bring the school's reputation into disrepute;
- Follow the school's Mobile Phone and Devices policy;
- Report any concerns about a pupil related to safeguarding and e-safety to the Designated Safeguarding Lead;
- Report accidental access to inappropriate materials to the ICT Manager so that inappropriate sites are added to the restricted list;
- Only use school owned devices and memory cards to take photographs or videos;
- Undertake refresher online safety training at least once each academic year which includes their expectations, roles and responsibilities around filtering and monitoring systems.

Inappropriate Use by Staff

If a member of staff is believed to have misused the internet or network in an abusive or illegal manner at school, a report must be made immediately to the Headteacher and ICT Manager. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary.

Refer to Annex 1 for further guidance.

Parents and Visitors

All parents have access to a copy of this Online Safety Policy on our website. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

As part of the approach to developing online safety awareness with pupils, the school may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using online technologies beyond school; this may be by offering parent education sessions or by providing advice and links to useful websites. The school wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

Parents should be aware that the school cannot take responsibility for a pupil's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other pupils, and the possibility of pupils accessing inappropriate content. However, should parents or guardians become aware of an issue, we strongly encourage prompt communication with the school so we can offer advice and support. The school has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

Video and Photography at School Events

Parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of other children in any public forum without the permission of the relevant family.

Early Years Use of Mobile Phones or Device - Statutory Regulation

The Early Years Safeguarding and Welfare Requirements (para 3.4) requires all schools to have a clear policy on the use of mobile phones and devices.

Code of Conduct for Staff states, that Staines Prep does not permit the use of personal mobile phones and cameras by staff where children are present.

The School's Responsibilities

The school takes its responsibilities in relation to the acceptable use of technology by pupils and adults seriously and understands the importance of monitoring, evaluating and reviewing its procedures regularly.

Filtering and Safeguarding Measures

The school's internet has a robust filtering and monitoring system (Smoothwall) which is set at an age-appropriate level such that inappropriate content is filtered and is reviewed regularly, to ensure that children are safe from terrorist and extremist material (as required by the Prevent Duty) and inappropriate material when accessing the internet at School. Advice has been taken from [UK Safer Internet Centre: appropriate filtering and monitoring](#). The system logs all attempts to access the internet, including all attempts to access inappropriate content and a report is sent directly to the ICT Manager and Headteacher.

Anti-virus, anti-spyware, junk mail and SPAM filtering is used on the school's network, stand-alone PCs, laptops and tablets, and is updated on a regular basis. Security measures are in place to ensure information about our pupils cannot be accessed by unauthorised users. Strong encryption is used on the wireless network to provide good security.

Email Use

Pupils are given access to suitable e-mail and messaging facilities when the curriculum covers this topic. Expectations and safety measures are covered during this time.

All staff are expected to use email professionally and responsibly. See Annex 3 for further details.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Staines Prep recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Staines Prep will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

The School's Use of Images and Videos

The school abides by data protection legislation and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes, such as a yearbook. Parents and guardians may withdraw their permission at any time by informing the school in writing.

Staff are not permitted to use their own devices or memory cards to record videos or photographs of pupils, and when storing images within the school's network are requested to only use the pupil's first name.

The Curriculum and Tools for Learning

The school teaches our pupils how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through ICT and/or PSHE lessons. The PSHE curriculum supports the teaching of online-safety and further guidance for teaching content is found at [Education for a Connected World](#) and [Be Internet Legends](#). The following concepts, skills and competencies are taught through the school in an age-appropriate manner:

- Digital citizenship;
- Future work skills;
- Internet literacy;
- Making good judgments about websites and emails received;
- Knowledge of risks such as viruses, and opening mail from a stranger;
- Access to resources that outline how to be safe and responsible when using any online technologies;
- Knowledge of copyright and plagiarism issues;
- Awareness of age restrictions on common social media sites and games;
- Positive online communication which is not harmful or upsetting for others;
- Sharing personal information about themselves or others;
- File-sharing and downloading illegal content;
- Uploading information – knowing what is safe to upload, and not to upload personal information; and

- Where to go for advice and how to report abuse.

These skills are taught explicitly within the ICT curriculum but are likely to be covered in other subjects; pupils are taught skills to explore how online technologies can be used effectively, in a safe and responsible manner. Further details about the content of the curriculum related to ICT can be found in the ICT and PSHEE curriculum documentation.

Monitoring

It is the responsibility of the school, including the governing body to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the school network. The school will monitor the use of online technologies and the use of the internet by pupils and staff.

Social Media

Access to social networking sites is not permitted in school. However, the school will advise pupils about their safe use e.g. use of passwords and appropriate age limits. Staff have received training on child-on-child abuse and Sexual Violence and Harassment in schools to develop their awareness of identifying concerning behaviours which may be linked to this issue. Staff are also aware of guidance surrounding making or sharing nudes/semi-nudes. The training ensures that staff know how to respond to concerns in line with the school's Child Protection and Safeguarding policy.

Cyberbullying – Definition

Cyber bullying can be defined in the following terms:

Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others.

Cyberbullying can involve Social Networking Sites, emails and mobile phones, used for SMS messages and as cameras.

The DfE advice *Preventing and Tackling Bullying 2014* states that:

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.

Cyberbullying – Preventative Measures

We expect all pupils to adhere to our Computing Acceptable Use Policy for the safe use of the internet. This policy has been created to offer guidelines for pupils using Computing, and the Computing Curriculum address e-safety, helping to generate a culture of awareness for cyberbullying.

Our Computing Department monitors pupils' use.

We may impose sanctions for the misuse, or attempted misuse of the internet.

We offer guidance on the safe use of social networking sites and cyberbullying in Computing lessons.

We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe.

Cyber-bullying will be covered in PSHEE lessons and during a focused Anti-Bullying week.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the DSL (or a deputy), will consider a referral into the [Cyber Choices](#) programme.

This programme aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Mobile phones are not permitted in the School. In exceptional circumstances pupils, with the agreement of the Headteacher, pupils may leave mobile phones with the Reception Office.

Annex 1 - Procedures for staff in the event of a breach of this policy by a pupil or adult

- (A)** An inappropriate website is accessed inadvertently:
- Ensure that no one else can access the material, by turning off the screen;
 - Record the incident in writing using the school's pro forma;
 - Report to Headteacher; and
 - Contact ICT Manager so that it can be added to the banned or restricted list.
- (B)** An inappropriate website is accessed deliberately:
- Ensure that no one else can access the material, by turning off the screen;
 - Record the incident in writing using the school's pro forma;
 - Report to the Headteacher and ICT Manager immediately; and
 - The Headteacher applies the Behaviour Policy.
- (C)** An adult receives inappropriate material:
- Do not forward this material to anyone else – doing so could be an illegal activity;
 - Alert Headteacher and DSL immediately; and
 - Ensure the device is shut down and record the nature of the material.
- (D)** An adult has used ICT equipment inappropriately:
- Follow the procedures for (B).
- (E)** An adult has communicated with a pupil, or used ICT equipment, inappropriately:
- Ensure the pupil is reassured;
 - Report to the Headteacher who should follow the Staff Code of Conduct and Safeguarding Policy (if relevant);
 - Preserve the information received by the pupil if possible, and determine whether the information received is abusive, threatening or innocent; and
 - If illegal or inappropriate use is established, contact the Headteacher (or the Chair of Governors), if the allegation is made against the Head) and the Designated Safeguarding Lead immediately, and follow the Safeguarding Policy.
- (F)** Threatening or malicious comments are posted to the school website or distributed via the school email system (or printed out) about an adult in school:
- Preserve any evidence; and
 - Inform the Headteacher immediately and follow the Safeguarding Policy as necessary.
- (G)** Where images of staff or adults are posted on inappropriate websites, or have inappropriate information about them posted anywhere:
- The Headteacher should be informed.

Annex 2 - Computing Acceptable Use Policy for Pupils

Our school has provided digital equipment, such as iPads, computers and Internet access to help you learn. You are responsible for your own behaviour on the Internet, just as you are in a classroom or the playground. Our Internet access is filtered to screen undesirable sites to protect you and the School, and the system can also scan e-mails for viruses

These rules will help keep everyone safe:-

- You must ask permission from a teacher before using any digital equipment. You must use the digital equipment only for schoolwork and homework.
- Do not eat or drink near digital equipment.
- Do not bring in CDs or USB memory devices from outside school, unless permission is given by a teacher. You may only access the network using your own login.
- When using the Internet, to help protect other pupils and yourself, tell a teacher if you see anything you are unhappy with. Turn the screen off, if something upsets you.
- Do not download files or print from the Internet unless a teacher gives permission.

- Do not fill in personal details on web pages, enter competitions or visit chat rooms.

E-mail and Messaging

- You will be given access to suitable e-mail and messaging facilities when the curriculum covers this topic. You must only e-mail/message people your teacher has approved.
- The messages you send must be polite and sensible.
- Do not give personal details, your home address or telephone number.
- Any time you use e-mails/messaging, if you receive a message which you do not like, you must tell a teacher.
- Any time you are online, you must never arrange to meet someone. Tell a teacher if someone asks to meet you. Unsafe people can pretend to be friendly.

Mobile Phones

- Mobile phones are not allowed in school, but the rules above will also help to keep you safe when using them at home.

Learning Platform – RMUnify

RMUnify is accessed using the school network login details and provides a single sign on facility to access a range of learning programs as well as work through OneDrive. The activities on RMUnify are intended for your sole use. You may request support from a responsible adult, where necessary.

- You must keep your RMUnify login details secret.
- You must only access RMUnify using your own login.
- At school, you may only upload files/images to RMUnify if a teacher gives permission.
- At home, you may only upload files/images to RMUnify if approved by an adult.

The School reserves the right to withdraw your access to RMUnify should it be found that it is being misused either deliberately or through carelessness.

Please remember that the school may check your computer files and can monitor the Internet sites you visit.

Annex 3 – Email Etiquette

Email best practice

- Write well-structured emails and use short, descriptive subjects.
- Sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. The use of internet abbreviations and characters such as smileys is not encouraged.
- Signatures must include your name, job title and school name. A disclaimer should be added underneath your signature.
- Users must spell check all mails prior to transmission.
- Only mark emails as important if they really are important.
- Avoid long strings of messages; start new conversations.

Do not

- Write it in an email unless you would put it on a noticeboard in the office or in a newspaper.
- Write anything that is libellous, defamatory, offensive, racist or obscene - you and the school can be held liable.
- Forward confidential information - you and the school can be held liable.
- Forward a message with sensitive information without acquiring permission from the sender first.
- Send email messages using another person's email account.

Annex 4 – Useful resources

Organisation/Resource	What it does/provides
Think-u-know	NCA CEOPs advice on online safety
Disrespect nobody	Home Office advice on healthy relationships, including youth produced sexual imagery and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
SWGFL	Provides advice on all aspects of a school or college's online safety arrangements
Internet Matters	Help for parents on how to keep their children safe online
Parentzone	Help for parents on how to keep their children safe online
Childnet cyberbullying	Guidance for schools on cyberbullying
PSHE association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
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.
Educate against hate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
The 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
UKCIS	The UK Council for Internet Safety's website provides: <ul style="list-style-type: none"> • 'Sharing nudes/semi-nudes' advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
Net-aware	NSPCC advice for parents
Common sense media	Independent reviews, age ratings, & other information about all types of media for children and their parents
Searching Screening and Confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
LGFL	Advice and resources from the London Grid for Learning
Teaching online safety in school	Departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.