Online safety policy

KTS ACADEMY

Approved by:	Sarah Gunn	**Date:**	10.19.26
Last reviewed on:	10.9.26		
Next review due by:	10.9.27		

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents/carers about online safety
6. Cyber-bullying
7. Acceptable use of the internet in school
8. Pupils using mobile devices in school
9. Staff using work devices outside school
10. How the school will respond to issues of misuse
11. Training
12. Monitoring arrangements
13. Links with other policies

Appendices:

- Appendix 1: Formal and semi-formal curriculum pupils (main site) acceptable use agreement
- Appendix 2: Formal curriculum pupils and post 16 (KTS+) acceptable use agreement
- Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)
- Appendix 4: Filtering and monitoring arrangements

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, misandry, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as making or sharing of nudes or semi-nudes (including images digitally altered or wholly generated by artificial intelligence), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education (2026), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation
- Mobile phones in schools
- Generative artificial intelligence in education

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 takes into account the National Curriculum computing programmes of study.

This policy complies with data protection legislation, which collectively encompasses the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), and the Data (Use and Access) Act 2025.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

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

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

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will review their effectiveness at least once every academic year. This review must be conducted by the Senior Leadership Team (SLT) member responsible for filtering and monitoring, supported by the Designated Safeguarding Lead (DSL) and IT support.

The board will review the DfE's 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

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 (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college 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

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy 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:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board 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 provider to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT provider 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 board
- 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.

3.4 ICT Management

ICT support is provided by One IT, who support in:

- Putting in place an appropriate level of security protection procedures, including 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

More information about filtering and monitoring can be found in Appendix 4.

The designated safeguarding lead (DSL) is responsible for:

- Ensuring that any online safety incidents are logged on CPOMS 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.

3.5 All 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 failing by informing the DSL immediately
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS (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
- 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.

3.6 Parents/carers

Parents/carers are expected to:

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

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.7 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.

3.8 Volunteers

All volunteers are expected to:

- Maintain an understanding of this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

Volunteers and regulated activity:

Any volunteer who frequently teaches, trains, instructs, or supervises children is legally in regulated activity and requires an enhanced DBS check with children's barred list information. This requirement applies regardless of whether the volunteer is supervised by a person in regulated activity.

This is in accordance with The Crime and Policing Act 2026 and KCSIE 2026.

The headteacher and DSL are responsible for ensuring all volunteers working with children have appropriate checks in place before beginning their role.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of their curriculum, within Computing and Relationship and Sex/Health Education. The curriculum has been carefully designed to ensure pupils learn about online safety in a way that is appropriate to their level of understanding and individual needs. The curriculum aims to:

- Give pupils the knowledge and behaviours that pupils need to help them navigate the internet safely
- Help pupils understand the harms and risks associated with being online
- Teach them the importance of looking after their wellbeing when using the internet

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or via ClassDojo, and in information via our website or Facebook page.

Online safety training will also be offered annually.

The school website informs parents:

- What systems the school uses to filter and monitor online use
- What pupils will be learning about online as part of their curriculum

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

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be during lessons, including personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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

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

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or member of the senior leadership team
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude, including AI-generated or AI-altered images), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and guidance on making or sharing of nudes or semi-nudes

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- Guidance on making or sharing of nudes or semi-nudes
- KTS Behaviour policy

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

6.4 Artificial intelligence (AI)

Generative 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 Gemini.

KTS Academy recognises that AI has many uses to help pupils learn, but also has the potential to be misused in harmful ways, including:

- Creating 'deepfakes' – AI-generated images, audio or video hoaxes that look real
- Deepfake pornography – pornographic content created using AI to include someone's likeness without consent
- AI-generated or AI-altered nudes or semi-nudes of children

KTS Academy will treat any use of AI to bully pupils or create inappropriate images very seriously, in line with our behaviour policy and child protection policy.

All incidents involving AI-generated or AI-altered nudes or semi-nudes will be treated as safeguarding incidents and will mandate a safeguarding response, regardless of whether the images are of real children or digitally created.

Staff must be aware of the safeguarding, data protection, and ethical risks involved in the educational use of Generative AI and should carry out a risk assessment where:

- New AI tools are being introduced
- Existing AI tools are used in cases which may pose a risk to pupils or staff

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

7. Acceptable use of the internet in school

Pupils (where appropriate) and all parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

KTS Academy operates as a mobile phone-free environment. Pupils may bring mobile devices into school, but they must hand them in when they arrive and they are stored away securely until the end of the day.

This policy is in line with DfE guidance on mobile phones in schools, which establishes that schools should be mobile phone-free environments to support pupil wellbeing, behaviour and learning.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy.

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from One IT.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will determine the action on a case-by-case basis. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Making or sharing of nudes or semi-nudes (including AI-generated or AI-altered images), especially around chat groups
    - Sharing of abusive images and pornography to those who don't want to receive such content, including AI-generated content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

Teachers log behaviour and safeguarding issues related to online safety on CPOMS and they are then actioned.

This policy will be reviewed every year by the deputy headteacher. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- AI usage policy

Appendix 1: Pupils following the formal or semi-formal curriculum (main site)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS
Name of pupil:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS	

When I use the school's ICT systems (like computers or Ipads) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
• I find anything that may upset or harm me or my friends
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**

Appendix 2: KTS+ pupils

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will hand it in when I arrive in school **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
• When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school • I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Filtering and monitoring arrangements

Securly Filter is a web filter designed for schools and widely deployed in the UK and around the world. As UK government guidance evolves Securly makes every effort to ensure that its products comply and help schools comply with their statutory obligations around student safety and well-being.

filter

Securly Filter is one of a suite of school focused safety products from Securly designed to make it seamless for schools to meet their student safety obligations. Specifically, Securly Filter meets the filtering technical requirements, and Securly Aware and Securly Classroom help schools meet their KCSIE monitoring obligations.

Responses to KCSIE Web Filter Requirements

Make sure your filtering provider is:

KCSIE GUIDANCE	SECURLY RESPONSE
A member of Internet Watch Foundation (IWF).	Securly has been an IWF member since 01/03/2016.
Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU).	Securly receives and incorporates the CTIRU feed into its filtering technology.
Blocking access to illegal content including child sexual abuse material (CSAM).	Securly blocks access to illegal content including CSAM.
If the filtering provision is procured with a broadband service, make sure it meets the needs of your school or college.	Securly works with broadband providers and managed service providers to ensure Securly Filter is well configured and fit for purpose.

Your filtering system should be operational, up to date and applied to all:

KCSIE GUIDANCE	SECURLY RESPONSE
Users, including guest accounts.	Securly Filter can be applied to all device types and all user categories in all locations, with user-level logging and filtering through sign-in and directory integration with Microsoft Azure or Google G-Suite. Securly's cloud architecture supports all device types (Windows, Chrome, iOS, MAC, Android, etc.) in all locations (in and away from school). It supports school-owned devices, guest networks, and BYOD.
School-owned devices.	Securly Filter can be applied to the school network, filtering all devices on the network and to individual school owned devices, of all types, including but not limited to windows, chrome, iOS, Android, Linux. School owned devices can then be filtered in any location.
Devices using the school broadband connection.	Securly Filter can also be applied to BYOD devices, and Guest networks ensuring all devices using the school broadband connection are appropriately filtered.

Your filtering system should:

KCSIE GUIDANCE	SECURLY RESPONSE
FIlter all internet feeds, including any backup connections.	Securly Filter can be applied at both the user/device level and at the network level.
Be age and ability appropriate for the users, and be suitable for educational settings.	Securly Filter is built exclusively for education and has school appropriate filtering configured out-of-the-box with simple configuration of more strict or relaxed policies as required. Through manual configuration or directory integration age appropriate (and other group) settings may be implemented.
Handle multilingual web content, images, common misspellings and abbreviations.	Securly Filter and it's classification engine PageScan (incorporation text scan and image scan) use dynamic categorisation, crowd sourced URL scanning, search engine crawling and paid 3rd party categorisation to keep its classification database up to date and to dynamically categorise new sites. This is an industry standard approach which covers text and images, is multilingual and handles common abbreviations and misspellings.
Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.	Securly works with schools to ensure Securly Filter is applied in the most robust way possible and includes publicly available best practice guides and recommendations for configuring devices and networks to best protect children and prevent circumvention.
Provide alerts when any web content has been blocked.	Securly Filter includes the ability to generate instant alerts for blocked content, this is configurable at a policy level to allow for different alert levels for vulnerable users.
Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.	Securly Aware connects directly into Microsoft Office365 and G-Suite Workspace to scan documents, emails, chats, images, and videos for inappropriate content regardless of where those systems are used or how they are accessed.
It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.	Securly Filter categorises blocked URLs in a way designed to be useful in schools, Categories include pornography, drugs, gambling, hate and other adult. Students trying to access unsuitable material will be blocked, an alert is generated and the activity logged against the student. Appropriate staff may investigate via the reporting system.

Your filtering systems should allow you to identify:

KCSIE GUIDANCE	SECURLY RESPONSE
Device name or ID, IP address, and where possible, the individual.	Securly Filter logs the username from Microsoft Azure AD or G-Suite; for shared devices, a device name or serial number may be used instead, or where authentication is not possible, an IP address is recorded. This information determines if a device or user is on-site or off-site and if policies should differ based on that measure.
The time and date of attempted access.	The search term or content being blocked by Securly Filter and Securly Aware is logged and includes a date and timestamp for all activities.
The search term or content being blocked.	Securly Filter logs search terms in a format that is easy for non-technical users to inspect and understand.

ONE IT
SERVICES & SOLUTIONS

Prefer to talk?
01642 635570