



Online Safety Policy

5th September 2025



Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying	7
7. Acceptable use of the internet in school	9
8. Pupils using mobile devices in school	10
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse	10
11. Training	11
12. Monitoring arrangements	11
13. Links with other policies	12
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers).....	13
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers).....	14
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors).....	15
Appendix 4: online safety training needs – self-audit for staff.....	16
Appendix 5: Provider Response – KCSIE Guidance, Filtering and Monitoring	17
Appendix 6: Academy Filtering and Monitoring Procedures.....	23

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, local governors and trustees.
- 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, 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, 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

2. 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](#)
- [Relationships and sex education](#)
- [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 takes into account the National Curriculum computing programmes of study.

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

3. Roles and responsibilities

3.1 The Local Governing Board

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

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

The local governing board 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 board will review the DfE filtering and monitoring standards, inline with the [DfE's Filtering and Monitoring Standard 2025](#) and discuss with IT staff and service providers what needs to be done to support the school in meeting these standards, which include:

Belonging Believing Becoming

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually and risk assessed in-line with evolving threats.
- Make use of tools such as [UK Safer Internet Centre](#) webinars and [TestFiltering.com](#)
- 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 DDSL are set out in each school's Child Protection Policy and Safeguarding Policy.

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 local 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 manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, 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 on CPOMS 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 local 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 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 meet the [DfE Cyber Security Standards for Schools and Colleges](#) and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct annual reviews of cybersecurity procedures and include staff awareness training on phishing, ransomware, and data protection.
- Conducting full security checks and monitoring the school's ICT systems as outlined in appendix 7
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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 Academy Trust Board immediately.

Belonging Believing Becoming

- Following the correct procedures by working closely with their ICT provider/manager if they need to bypass the filtering and monitoring systems for educational purposes but ensuring permission is granted by the DSL and Headteacher.
- Working with the DSL to ensure 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
- 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.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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 International](#)
- Parent resource sheet – [Childnet International](#)

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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- [Relationships education and health education](#) in primary schools in line with the revised [RSHE guidance 2026](#).
- [Relationships and sex education and health education](#) in secondary school

In **Key Stage (KS) 1**, pupils will be taught to:

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

Pupils in **Key Stage (KS) 2** will be taught to:

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

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

All schools –

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

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

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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 1 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. Teachers will discuss cyber-bullying with classes.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (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 behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will 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 and DSL.
- 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 Headteacher 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 image), 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 the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy / searches and confiscation 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 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.

Thrive CE Academy Trust 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.

Thrive CE Academy Trust will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Thrive CE Academy Trust's 'AI Policy' outlines how AI should be used safely within schools via the Trust Office 365 and Google tenancy. This is in line with the [DfE's Generative AI Product Safety Expectations \(2025\)](#). Staff adhere to this policy at all times.

7. Acceptable use of the internet in school

All pupils, 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

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

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 the school's IT provider/manger and inform the Headteacher and DSL.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 code of conduct policy. 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
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such 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 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

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the Trust Board. At every review, the policy will be shared with the local governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly. This annual risk assessment reflects the 4Cs of online risk (Content, Contact, Conduct, Commerce) and is informed by monitoring logs, incident reports, and staff feedback.

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
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

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

Name of pupil:

When I use the school's ICT systems (like computers) 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
- Use school computers for school work only
- 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
- Save my work on the school network
- 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:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

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 not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

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: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school’s acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school’s devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school’s ICT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Provider Response – KCSIE Guidance, Filtering and Monitoring



The Department of Education Keeping Children Safe in Education (KCSIE) 2023 Statutory Guidance firmly puts the responsibility for the provision and operation of web filtering and monitoring solutions on school leadership rather than on the IT team.

- School governing bodies and proprietors have overall strategic responsibility for filtering and monitoring.
- SLTs are responsible for procuring filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of filtering provision, and overseeing reports.
- SLTs and DSLs have a responsibility to understand filtering and monitoring systems.

Securly's Securly's Safety and Wellness ecosystem makes Filtering and Monitoring Compliance easy.

With cloud based web filtering and monitoring powered by its market leading AI, Securly prevents access to inappropriate websites, provides alerts on detected student safety issues, monitors student wellness levels, and allows teachers to monitor student activity on devices in class. Throughout the solution there is focus on minimising staff workload whilst identifying at risk students and enabling early intervention.

For more information, or a product demonstration, please contact us:

0800 862 0126

www.computeam.co.uk



Built for Education, Designed for Schools.	➤ Securly's suite of solutions is built for and sold exclusively to schools. These intuitive and easy-to-use products are designed for use by teaching staff and DSLs.
Delegated Administration	➤ Securly's delegated administration options give teaching staff direct access to web filter policy management, alerts, and wellness dashboard data. Securly Filter and Aware are configurable to ensure staff only receive access to information on students that they are responsible for, reducing unnecessary work and keeping data secure.
Filtering and Monitoring Any Device Anywhere	➤ Securly's cloud architecture supports all device types (Windows, Chrome, iOS, MAC, Android, etc.) in all locations (in school and away from school). It supports school-owned devices, guest networks, and BYOD.
Student Safety Alerts	➤ Securly Aware uses the industry's longest-learning AI to examine student internet activity across searches, social media, web browsing, email, chat, and shared documents. It identifies potential issues such as bullying, violence, self-harm, grief, and suicide and notifies DSLs instantly.
Monitoring Wellness Levels	➤ Securly Aware conducts a real-time analysis of student activity to understand if they're showing signs of distress and assigns a reliable, real-time wellness level. ➤ Wellness level scores provide a simple indication of an individual students' state of mind and direction of change, enabling DSLs to understand which students require immediate intervention.
Monitoring Devices	➤ Securly Classroom provides cloud-based classroom management, enabling teachers to see student screens in a class session. This helps teachers guide lessons, monitor student progress, and keeps the focus on learning.

Any automated alert system has the potential to deliver too many alerts and false positives. Securly's AI and configuration options minimise false positives and reduce staff workload.

Minimising Staff Workload

By examining whole sentences rather than key words and using "sentiment analysis" to identify negative context, Securly minimises false positives. The alert triggers can also be customised for different groups of students, increasing or decreasing the level at which an alert is triggered.

Outsourcing Alert Monitoring and Investigation with On-Call

Schools rely on On-Call to help identify and respond to students at risk of self-harm, suicide, bullying, and violence. The On-Call Team analyses alerts from Securly Aware and notifies school staff immediately to ensure that alerts are followed up in the shortest possible timescale, leaving teachers free to teach!

For more information, or a product demonstration, please contact us:

0800 862 0126

www.computeam.co.uk





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.



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.
School-owned devices.	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.
Devices using the school broadband connection.	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.
	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 its 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.

For more information, or a product demonstration, please contact us:

0800 862 0126

www.computeam.co.uk





KCSIE guidance says that "monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software".

"A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:"

- ➔ Physically monitoring by staff watching the screens of users.
- ➔ Live supervision by staff on a console with device management software.
- ➔ Network monitoring using log files of internet traffic and web access.
- ➔ Individual device monitoring through software or third-party services.

Securly suite of safety and wellness solutions helps you meet these requirements.

Securly *Aware* is a student safety and wellness solution that provides unprecedented visibility into your students' mental health and wellness. The data provided by Aware can help you understand and meaningfully impact your students' wellness. With Aware, you can:



- ➔ Know who's at risk of self-harm, suicide, depression, violence, and bullying.
- ➔ Gain a clear picture of each student's current wellness level.
- ➔ React quickly with AI generated instant alerts on student safety issues.
- ➔ Identify student behavioral trends to intervene before a crisis occurs.
- ➔ Proactively support students who demonstrate concerning behaviours.
- ➔ Respond effectively to student safety concerns.

Securly *Classroom* enables teachers to monitor all of the devices in their class at once by displaying a thumbnail of each screen on a teacher's device and enabling teachers to zoom in on any particular student.



Responses to KCSIE Monitoring Requirements

KCSIE GUIDANCE	SECURLY RESPONSE
<p>Physical Monitoring Physical monitoring can contribute where circumstances and the risk assessment suggests low risk, with staff directly supervising children on a one-to-one ratio whilst using technology.</p> <p>Internet and web access Some Internet Service Providers or filtering providers provide logfile information that details and attributes websites access and search term usage against individuals. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches.</p> <p>Monitoring Content Recognising that no monitoring can guarantee to be 100% effective, schools should be satisfied that their monitoring strategy or system (including keywords if using technical monitoring services) at least covers the following content.</p> <p>Active monitoring where a system generates alerts for the school to act upon.</p> <p>Pro-active monitoring where alerts are managed or supported by a specialist third-party provider and may offer support with intervention. Proactive monitoring is most effective where?</p>	<p>Classroom Physical monitoring of devices on a 1:1 basis is time consuming and can be counterproductive to teaching and learning. Securlly offers Classroom, a system that enables teachers to monitor all the devices in their class at once by displaying a thumbnail of each screen on a teacher's device and enabling teachers to zoom in on any particular student.</p> <p>Filter. Delegated Admin. Securlly Filter offers delegated administration enabling teachers and student safety staff to access filter logs and reports on students in their care. The interface is simple and non-technical. Reports can be customised, accessed at any time, or scheduled.</p> <p>Aware Aware helps schools monitor search, web browsing, and web based social media. And email, documents, drives, messaging, in Google and Microsoft environments. A sophisticated AI engine uses keywords and sentiment analysis to identify and categorise harmful activity. All categories identified in the technical guidance are covered.</p> <p>Aware generates real time alerts which are sent to the appropriate staff. Alerts may be tuned to minimise staff workload.</p> <p>On-Call On-Call is a proactive monitoring service which utilises Securlly's trained student safety team to analyse alerts and respond by logging cases and managing appropriate escalations.</p>

For more information, or a product demonstration, please contact us:

0800 862 0126

www.computeam.co.uk



Appendix 6: Academy Filtering and Monitoring Procedures

Filtering

I.T Provider: Computeam

Filtering Software: Securly

Overview:

Weekly report generated and sent to Headteacher/DSL. This report will identify

1. Blocked Web Users
2. Blocked Web Categories
3. Blocked Web Domains
4. Blocked Web Hosts
5. Blocked Web Applications
6. Blocked Allowable Categories
7. Blocked Allowable Domains
8. Blocked Policies

These reports will identify the time and specific machine which has tried to access content.

Monitoring

All Schools

Monitoring Type: Physical Monitoring/Securly Aware

Overview:

Each user has their own log on which will identify which device has been used, by whom at what time. 'Aware' helps schools monitor searches, web browsing and social media. AI engines within 'Aware' identify and categorise harmful content and generate immediate alerts to the Headteacher/DSL.

When pupils are using IT equipment, it is also important that staff maintain physical monitoring whilst the pupils are working.

Reporting

All schools will adhere to this policy and ensure that staff have up to date training regarding internet safety, filtering and monitoring. All concerns will be dealt with inline with the relevant safeguarding policy or code of conduct policy for staff. CPOMS will be used to record all safeguarding concerns, including those linked to internet safety.