Document Title:	**Online Safety Policy**
Date of ratification by Trust Board (if applicable)	September 2026
Author:	Andrew Chadwick
Contributors:	
Version:	2.2
Date of Production:	June 2024
Latest review date:	September 2026
Amendment details (if applicable)	• Updated inline with KCSIE 2026 • Added a table at the front for schools to personalise
Review period	Annually or if guidance changes
Post holder responsible for revision:	SAIL
Primary Circulation List:	All staff, board members, school governors
Identify if policy is on FT web site or School web site	
Related Policies:	• Child protection and safeguarding policy • Behaviour policy • Staff disciplinary procedures • Data protection policy and privacy notices • Complaints procedure • ICT and internet acceptable use policy • Staff Code of Conduct • AI Policy

Contents

School Online Safety and Digital Safeguarding Profile 3
IT and online safety policy 3
1. Aims 3
The 4 key categories of risk 3
2. Legislation and guidance 4
3. Roles and responsibilities 4
4. Outside of school 8
5. Educating pupils about online safety 8
5.2 Cyber Security Education 9
6. Educating parents/carers about online safety 9
7. Cyber-bullying 10
8. Acceptable use of the internet in school 12
9. Pupils using mobile devices in school 12
10. Staff using work devices outside school 13
11. How the school will respond to issues of misuse 13
12. Training 14
13. Monitoring arrangements 14
Appendix 1: online safety training needs – self-audit for staff 16

School Online Safety and Digital Safeguarding Profile

Designated Safeguarding Lead (DSL)	
Deputy DSLs	
Named Safeguarding Governor	
IT support provider	
Filtering provider	
Monitoring provider	
Broadband / Internet provider	
Date of last filtering review	
Date of last monitoring review	

IT and online safety policy

1. Aims

Focus-Trust 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
- 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, misinformation, disinformation, conspiracy theories, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, deepfake content, AI-generated harmful content and content designed to facilitate fraud or criminal exploitation
- **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, financial scams, cryptocurrency scams, online fraud, money mule recruitment and financial exploitation

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
- 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.

This policy also reflects the DfE Filtering and Monitoring Standards and relevant guidance issued by the UK Safer Internet Centre and the National Cyber Security Centre (NCSC).

This policy links closely with the Focus-Trust Child Protection and Safeguarding Policy.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 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, Teams 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, through the Named Safeguarding Governor's NSG Planner tool, 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 LGB 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 the 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.

The Named Safeguarding Governor oversees online safety.

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 through school and additional policies and 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 / principal

The headteacher / principal 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 (DSL)

Details of the school's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSLs) 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

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Computing Lead / IT Technician to make sure the appropriate systems and processes are in place
- Working with the headteacher, Computing Lead/ IT Technician 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 (on CPOMs) and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (see an optional self-audit for staff on online safety training needs, in appendix)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher, governing body and Focus-Trust board, through the Safeguarding, Ambition and Inclusion Lead
- 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
- 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 half-termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files. **It should be noted that IT Technicians must not add websites or applications to a whitelist or allow list without prior approval from the DSL or Headteacher and appropriate risk assessment.**
- Complete a self-review tool, such as 360 Degree Safe - Online Safety Review Tool | SWGfL and share the results with the governing body. This should inform an action plan and next steps to be completed.
- Complete a review, using the DFE Tool, Plan technology for your school - GOV.UK which will give personalised recommendations for how to meet the filtering and monitoring standards

- Responding to safeguarding concerns identified by filtering and monitoring

This list is not intended to be exhaustive, and may need to be completed in conjunction with the headteacher / principal, Computing Lead, IT technician, School Business Manager etc.

3.4 All staff and volunteers

All staff, including contractors and supply 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 reporting any incidents of those systems or processes failing directly to the DSL, immediately
- Following the correct procedures by speaking to the DSL if they need to bypass the filtering and monitoring systems for educational purposes
- 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.

3.5 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

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

3.6 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, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Outside of school

We are aware that many children have unrestricted access to the internet outside of school. To address the implications of this, we have created a strong curriculum as well as a parent / carer education strategy, as identified in section 5 and 6 of this policy.

5. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

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
- Be discerning in evaluating digital content

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
- That many online services and apps collect personal information and may use this information for commercial purposes, including targeted advertising
- That social media platforms often have minimum age requirements and these are designed to help protect children from inappropriate content and unsafe contact

- That information encountered online may not always be accurate, trustworthy or genuine and that some images, videos and information may have been manipulated, including through artificial intelligence (AI)
- The risks associated with online scams, phishing attempts and requests for personal information
- How to identify and seek help if they experience pressure online to share personal information, images, videos or money
- 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
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

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.

5.2 Cyber Security Education

The school will provide age-appropriate education on cyber security, including:

- Creating and maintaining strong passwords
- Understanding multi-factor authentication
- Recognising phishing and scam messages
- Understanding social engineering techniques used by criminals
- Safe use of devices and removable media
- Protecting personal information online
- Reporting cyber incidents and security concerns to trusted adults

Cyber security education will be delivered through the computing curriculum and reinforced through wider safeguarding education.

6. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications, for example newsletters, posts on social media and sharing resources such as WakeUpWednesday. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings and other parent events such as workshops and assemblies.

The school wil 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.

7. Cyber-bullying

7.1 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. "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" – DfE Preventing and tackling bullying, July 2017, page 8.

7.2 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. It will be discussed as part of whole-school assemblies and by class teachers with their registration 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).

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.

7.3 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:
    - 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 headteacher 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 Headteacher) 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
- The school's behaviour policy
- The school's Child Protection and Safeguarding 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.

7.4 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 Co-Pilot.

Focus-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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Focus-Trust will treat any use of AI to bully pupils in line with the school's behaviour or 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, following all Trust advice and guidance.

Staff should refer to the Focus-Trust AI policy.

8. 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. 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.

9. Pupils using mobile devices in school

Older pupils may bring mobile devices into school, but must hand them to their teacher on entry to school. 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.

10. 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 can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager
- 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
- Ensuring that there is anti-virus and anti-spyware software installed, or requesting it from school
- 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.

Work devices must be used solely for work activities. In line with this, staff should be aware that this includes all IT systems, such as Microsoft 365 and as such the Trust email system should not be used for personal purposes and the "profile picture" if chosen to be used should be a professional current photograph (such as staff ID badge photo), school logo or left with no image.

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

11. 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 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 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.

12. 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, Teams posts 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, threatening, 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 and DDSLs will undertake child protection and safeguarding training, which will include online safety, in line with our Child Protection and Safeguarding Policy.

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.

13. Monitoring arrangements

Termly reports of Online Safety issues to the Trust board, termly. Schools to report to LGB termly.

Online safety, filtering and monitoring arrangements will be reviewed at least annually and reported to governors and trustees termly through safeguarding reporting processes.

This policy will be reviewed annually by the Safeguarding, Ambition and Inclusion Lead, or earlier if there is a change in guidance. At every review, the policy will be

shared with the Trust board and schools. Schools should also supplement this policy with their Safeguarding action plan, taking into account the outcomes of the SWGFL 360 tool.

Appendix 1: online safety training needs – self-audit for staff

Adapt this form to suit your needs.

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?	