Three Spires TRUST

'Life in all its fullness'

Online Safety Policy

Policy Owner	Director of Safeguarding & SEND
Approval by	Trust Board
Date approved	September 2024 Amended September 2025 – changes in green
Review date	September 2026

Contents:

Statement of intent

At Three Spires Trust, we understand that using online services is an important aspect of raising educational standards, promoting child achievement, and enhancing teaching and learning. The use of online services is embedded throughout our academies; therefore, there are a number of controls in place to ensure the safety of children, young people and staff.

This policy applies to all staff, pupils and all those who have access to the internet and use of technology provided by the Trust.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views. This also includes misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children and young people or young adults with the intention to groom or exploit children and young people.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect children and young people and staff revolve around these areas of risk. The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all children and young people and staff. The Trust recognises that online safety is a constantly evolving topic that emerges at a rapid pace. We aim to reduce online risks for the pupils in our Trust as set out in this policy.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children and young people safe in education 2025'
- DfE (2019) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- DfE (2014) Cyberbullying: Advice for Headteachers and school staff
- DfE (2022) Meeting digital and technology standards in schools
- DfE (2025) Generative artificial intelligence (AI) in Education

This policy operates in conjunction with the following trust-wide policies:

- Managing Allegations Against Staff (including low level concerns) Policy
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Searching, Screening and Confiscation Policy
- Staff Code of Conduct
- Data Protection Policy
- Confidentiality Policy
- Photography Policy
- AI policy

This policy operates in conjunction with the following policies that are local to individual academies:

- Child-on-child Abuse Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Behaviour Policy
- Disciplinary Policy and associated Procedures
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Acceptable Use Agreement for Children
- Acceptable Use Agreement – Staff

2. Roles and responsibilities

The trust board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Reviewing this policy on a biannual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.

- Ensuring that a member of staff in the central team's remit covers online safety.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant trust-wide policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Local Governing Body is responsible for:

- Ensuring that a member of staff in the academy's remit covers online safety.
- Ensuring that all staff members have read and adhere to this policy and the AUP
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that all relevant local policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Reviewing the DfE Filtering and Monitoring standards and ensuring there are roles in school to support meeting these standards

The Director of Safeguarding and SEND is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the trust's policies and procedures, including in those related to the curriculum, induction and safeguarding.
- Supporting the DSLs, their deputies and the academy colleagues with responsibility for online safety, by ensuring they are supported to carry out their responsibilities in relation to online safety.

The IT Business Partner is responsible for:

- Implementing appropriate security measures, such as filtering and monitoring systems on all school devices and networks
- Supporting ICT technicians to secure a safe learning environment.
- Working collaboratively with safeguarding teams both centrally and in schools, to promote a safe learning environment for children and young people
- Accessing regular and appropriate training to ensure they recognise current online safety risks

The principal is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the academy's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and their deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated at least annually.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all children and young people can develop an appropriate understanding of online safety.
- Organising engagement with parents and carers to keep them up-to-date with current online safety issues and how the academy is keeping children and young people safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Ensuring that there is appropriate monitoring and filtering in place for pupils in out of school settings e.g. alternative provision

The DSL is responsible for:

- Taking the lead responsibility for online safety in the academy.
- Working with the ICT teams to ensure that the appropriate monitoring and filtering systems are in place
- Undertaking training so they understand the risks associated with online safety and can recognise

additional risks that children and young people with SEND face online.
- Ensuring online safety is recognised as part of the academy's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the academy's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the academy's provision, and using this data to update the academy's procedures.
- Reporting to the governing board about online safety on a termly basis.

The identified member of staff in each academy with responsibility for online safety is responsible for:

- Acting as the named point of contact within the academy on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children and young people with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Working with the DSL to ensure that safeguarding is considered in the academy's approach to remote learning.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the academy's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the academy community understand the reporting procedure.
- Working with the principal, DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the online safety policies and procedures.
- Implementing appropriate security measures as directed by the trust ICT Business Partner.
- Ensuring that the academy's filtering and monitoring systems are applied, functioning correctly and updated as appropriate.
- Working with the DSL and principal to conduct half-termly light-touch reviews of this policy.
- Taking responsibility for their own CPD in this area

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that children and young people may be unsafe online.
- Reporting concerns in line with the academy's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Adhering to the Acceptable Use Agreement and other relevant policies.
- Engaging in and completing online safety CPD and having an awareness of current risks to young people

Children and young people are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Respecting the feelings and rights of others both online and offline
- Engaging in any online safety learning in the curriculum

Parents/carers are expected to:

- Support our online safety approaches by discussing online safety with their children and young people and reinforcing positive online behaviours

- Report any concerning online behaviours that could indicate their child may be at risk

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy where relevant, and will be expected to follow it. If appropriate, they will also be expected to agree to the terms of the Acceptable Use Policies.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children and young people using the internet.

The DSL has strategic oversight of each individual academy's approach to online safety, with the Online Safety lead having responsibility for the academy's approach to online safety, with support from deputies and the principal where appropriate, and will ensure that there are strong processes in place to handle any concerns about children and young people's safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across trust operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by children and young people to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that children and young people may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that children and young people displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children and young people's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the principal, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Managing Allegations against Adults Policy (including low level concerns), and Disciplinary Policy and Procedures. If the concern is about the principal, it is reported to the chair of governors.

Concerns regarding a child's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the principal and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy. This includes breaches of filtering and monitoring systems.

Where there is a concern that illegal activity has taken place, the DSL contacts the police.

The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the academy's response are recorded by the DSL. After serious concerns are investigated, we will identify any lessons learnt and evaluate our processes if required. We will share information with any relevant partner agency to reduce risk and to prevent abuse taking place online.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The academy will be aware that certain children and young people can be more at risk of abuse and/or bullying online, such as those who identify as LGBTQ+ and children and young people with SEND.

Cyberbullying against children and young people or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. To help prevent cyberbullying, we will ensure that children and young people understand what it is and what to do if they become aware of it happening, including to themselves or where they are a witness to it happening to others.

5. Child-on-child sexual abuse and harassment

Children and young people may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of academy, off and online, and will remain aware that children and young people are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to an academy culture that normalises abuse and leads to children and young people becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The academy will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other children and young people taking "sides", often leading to repeat harassment. The academy will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The academy responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the academy's premises or using academy-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that children and young people who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The child believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The child does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The child may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the child feel 'special', particularly if the person they are talking to is older.
- The child may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact children and young people are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the academy and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children and young people to behave in sexually inappropriate ways through the internet.

In some cases, a child may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children and young people are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children and young people to be groomed and manipulated into participating through the internet.

Where staff have any concerns about children and young people with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children and young people who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain children and young people at increased vulnerability to radicalisation, as outlined in Child Protection and Safeguarding Policy. Staff will be expected to exercise vigilance towards any children and young people displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a child relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Sextortion

Sextortion is a type of blackmail in which an individual manipulates or threatens to distribute explicit or intimate material (such as sexual images or videos) of the victim, unless certain demands are met. Children and young people are often targeted through online platforms and social media. Sextortion is the short name for ‘financially motivated sexual extortion’. Children and young people may be forced to pay money or do something else they do not want to.

Staff members are aware that sextortion attempts can happen very quickly or they can happen over a long period of time. Where staff have a concern that a child is at risk of, or has been a victim of sextortion, this must be reported to the DSL immediately. This will be investigated in line with the Child Protection and Safeguarding Policy.

7. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in children and young people, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of academy can have a substantial impact on a child's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a child is suffering from challenges in their mental health. Concerns about the mental health of a child will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the child and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst children and young people in the academy, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to children and young people, and whether the risk is one that is localised to the academy or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the principal will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing children and young people.
- Not inadvertently encouraging children and young people to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger children but is almost exclusively being shared amongst older children and young people.
- Proportional to the actual or perceived risk.
- Helpful to the children and young people who are, or are perceived to be, at risk.
- Appropriate for the relevant child's age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting children and young people at risk of harm, e.g. it encourages them to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant children and young people, e.g. those within a particular age range that is directly affected or even to individuals at risk where appropriate.

The DSL and principal will only implement a academy-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing children and young people's exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The academy will factor into its approach to online safety the risk that children and young people with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a child's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children and young people are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and online safety lead will ensure that children and young people are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that they cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on academy-owned devices or on academy networks through the use of appropriate firewalls.

10. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that children and young people are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life. All staff members should receive refresher training at least once each academic year as part of training or through relevant updates (staff meetings, online updates etc).

The DSL will undertake the relevant child protection training which includes online safety, at least every two years.

All new staff members (including Governors) will receive training as part of their induction on safe internet use and online safeguarding issues.

Information about the academy's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to a child's age and stage of development.

Children and young people are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours children and young people learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- That the same principles apply to online relationships as to face-to-face relationships, including the important of respect for others online
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks children and young people may face online are always considered when developing the curriculum.

The DSL is involved with the development of the academy's online safety curriculum. Children and young people will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The academy recognises that, while any child can be vulnerable online, there are some children and young people who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. children and young people with SEND and who are LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these children and young people receive the information and support they need.

The academy will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible indviduals, and in response to instances of harmful online behaviour from children and young people.

Teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of children and young people. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for children and young people?
- Are they appropriate for children and young person's developmental stage?

External visitors may be invited into the academy to help with the delivery of certain aspects of the online safety curriculum. The online safety lead and DSL decide when it is appropriate to invite external groups into an academy and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the teacher and DSL consider the topic that is being covered and the potential that children/young people in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any child who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a child who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the teacher ensures a safe environment is maintained in which children and young people feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything children and young people raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a child makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras
- Mobile phones
- AV1-robots (used in line with the separate Trust 'AV1 robot policy'

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that children and young people use these platforms at home, the class teacher always reviews and evaluates the resource. Teachers ensure that any internet-derived materials are used in line with copyright law.

Children and young people are supervised when using online materials during lesson time, whether this be in person or remotely – this supervision is suitable to their age and ability. All setting owned devices must be used in accordance with the Acceptable Use Policy, and any misuse will be dealt with in accordance with Behaviour Policy. Action taken will depend on the nature and seriousness of the specific incident.

The Trust firewalls will block inappropriate sites and apps on all school devices and network systems, to reduce this risk for pupils.

13. Use of smart technology

While the academy recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the academy will ensure it manages.

Children and young people will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the academy's Acceptable Use Agreement for Children.

Staff will use all smart technology and personal technology in line with the Staff ICT and Electronic Devices Policy.

The academy recognises that children and young people's unlimited and unrestricted access to the internet via mobile phone networks means that some children and young people may use the internet in a way which breaches the academy's acceptable use of ICT agreement for children.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Each academy has its own policy about the use of mobile phones; however, most ban children and young people's use of personal technology whilst on site.

Where there is a significant problem with the misuse of smart technology among children and young people, the academy will discipline those involved in line with the academy's Behaviour Policy.

Academy staff will lead assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The academy will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The academy will consider the 4C's (content, contact, conduct and commerce) when educating children and young people about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. The use of AI

The Trust has an AI policy that sets out guidelines for the ethical, secure, and responsible use of Artificial Intelligence (AI) technologies in our academy communities. The integration of AI technologies across our academies supports our Trust mission to 'reimagine education, equipping students with the skills they need to thrive in the 21st century'. However, we are aware that with any online platform, there are safeguarding risks that must be considered and that children's safety online is paramount.

The Trust Head of ICT and Systems has set clear guidelines for the safe and educational use of AI, working with the Director of Safeguarding and SEND, Assistant Director of Safeguarding, Director of Education and the academy Principals.

As with all online activity on an academy device, the use of AI is monitored by each academy's filtering and monitoring system, and any concerns are raised as per the procedures set out within our Child Protection and Safeguarding policy.

All staff will be made aware of the various ways in which children may be at risk using AI, including, but not limited to:

- Exposure to misinformation and disinformation
- AI generated indecent imagery of children
- Developing relationships with AI chatbots
- Online bullying and sexual harassment
- Potential extortion

Staff receive training on the risks of AI and the importance of reporting any concerns without delay.

15. Educating parents and carers

The academy works in partnership with parents and carers to ensure children and young people stay safe online both in the academy and at home. Parents and carers are provided with information about the academy's approach to online safety and their role in protecting their children. Parents and carers are sent

a copy of the Acceptable Use Agreement on an annual basis, and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents and carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of children, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.
- The rapidly developing use of AI

Parents and carers will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content. If parents/carers have any concerns in relation to online safety, these should be raised with the D(D)SL.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources
- Via individual academy's virtual learning environments

16. Internet access

Pupils, staff and other members of the academy community are only granted access to the academy's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access.

All members of the academy community are encouraged to use the academy's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Use of the internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual role. We will monitor websites visited by pupils and all staff (including volunteers and visitors) to ensure they comply with the above, and restrict access through our filtering and monitoring systems where appropriate.

17. Filtering and monitoring online activity

The LGB ensures 'over blocking' does not lead to unreasonable restrictions as to what children and young people can be taught with regards to online teaching and safeguarding.

The Principal, DSL and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. This has been implemented as per the expectations set out in KCSIE. The filtering and monitoring systems the academy implements are appropriate to children and young people's ages, the number of people using the network, how often children and young people access the network, and the proportionality of costs compared to the risks. ICT technicians undertake checks at least half-termly on the filtering and monitoring systems to ensure they are effective and appropriate.

Filtering

The Trust has ensured that each Academy has broadband connectivity through an appropriate provider. Academies are supported with this function by the Head of ICT and Systems.

Each Academy has the appropriate firewall and filtering systems in place to block inappropriate sites.

The filtering system identifies attempts to access inappropriate sites and categorises them. This includes (but is not limited to) self-harm, pornography, violence, racial hatred, gambling, extremism, gaming and sites of an illegal nature.

The system blocks all sites on the IWF list. When a concern regarding access to inappropriate sites is identified:

1) Staff member or pupil to report concern to the DSL and ICT technical team
2) Breach to be recorded as per policy and relevant staff informed
3) Parents/carers will be informed
4) Reports made to IWF, police or CEOP as appropriate
5) Review of both ICT equipment involved and filtering systems

Monitoring

The Trust has a duty to monitor internet use on all setting owned internet enabled devices. The following monitoring systems are in place across the Trust:

- St Regis - SENSO
- St Peters - SENSO
- The Kings, Kidsgrove - SENSO
- St Giles and St George's - SENSO
- St Thomas' - SENSO
- Hanley St Lukes - SENSO
- St Michaels' – Smoothwall
- Trust Central team - SENSO

Trust owned devices are monitored via SENSO when off site.

If a concern regarding pupil use of a device is identified via our monitoring arrangements, we take the appropriate steps in line with the safeguarding and child protection policy.

If a concern regarding pupil use of a device is identified via our monitoring arrangements, we will take the appropriate steps in line with the Child Protection and Safeguarding Policy, which may include:

1) Concern identified via monitoring system and received by key staff
2) Discussion with pupil (if appropriate)
3) Confiscation of technology/investigation (if required)
4) Concern to be recorded on My Concern/CPOMS
5) Parents/carers will be informed (if appropriate)

6) Review of pupil usage and understanding of online risks

Requests regarding making changes to the filtering system are directed to the Principal. Prior to making any changes to the filtering system, ICT technicians, the Principal and DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a child has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The academy's network and academy-owned devices are appropriately monitored. All users of the network and academy-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

18. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls at least fortnightly to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to ICT technicians.

All members of staff have their own unique usernames and private passwords to access the trust systems. Children and young people have their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords expire after 90 days, after which users are required to change them.

Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the principal is informed and decides the necessary action to take.

Users are required to lock access to devices and systems when they are not in use.

19. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Child Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

Staff and children and young people are given approved email accounts. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts are not permitted to be used on the academy site. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians. The academy's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown

sources are deleted without being opened.

20. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the academy. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff are not permitted to communicate with children and young people or parents/carers over social networking sites and are reminded to alter their privacy settings to ensure children and young people and parents or carers are not able to contact them on social media. Where staff have an existing personal relationship with a parent, carer or child, and thus are connected with them on social media, e.g. they are friends with a parent or carer at the academy, they will disclose this to the DSL and principal and will ensure that their social media conduct relating to that parent or carer is appropriate for their position in the academy.

Children and young people are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the academy community on social media are reported to the Principal and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Use on behalf of the academy

The academy's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the principal or the CEO to access the academy or trust social media accounts.

All communication on official social media channels by staff on behalf of the academy or trust is clear, transparent and open to scrutiny.

21. The academy website

The principal is responsible for the overall content of the academy's website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The central team will conduct regular compliance reviews – at least annually.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

22. Use of devices

Trust-owned devices

Staff members may be issued with the following devices to assist with their work:

- Laptop
- Tablet
- Mobile phone

Children and young people are provided with trust-owned devices as necessary to assist in the delivery of the curriculum,
e.g. tablets to use during lessons.

Trust-owned devices are used in accordance with the Device User Agreement. Staff and pupils are not permitted to connect trust-owned devices to public Wi-Fi networks. All trust-owned devices are password protected. All trust-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all trust-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians. Cases of staff members or children and young people found to be misusing trust-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

Personal devices

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are never permitted to use their personal devices to take photos or videos of children and young people.

Staff members report concerns about their colleagues' use of personal devices on the academy premises in line with the Managing Allegations Against Adults policy (including low level concerns). If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the principal will inform the police and action will be taken in line with the Managing Allegations Against Adults policy (including low level concerns).

Children and young people are not permitted to use their personal devices during lesson time or when moving between lessons. If a child needs to contact their parents during the school day, they are to make specific arrangements with a member of the safeguarding team. The principal may authorise the use of mobile devices by an individual child for safety or precautionary use.

Where a child uses accessibility features on a personal device to help them access education, e.g. where a child who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Children and young people's devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy. If a staff member reasonably believes a child's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Any concerns about visitors' use of personal devices on an academy's premises are reported to the DSL.

23. Monitoring and review

The trust recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the principal conduct at least half-termly light-touch reviews of this policy to evaluate its effectiveness.

The Trust Board, Director of Safeguarding and SEND, Assistant Director of Safeguarding and IT Business Partner review this policy in full on a biannual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2026.

Any changes made to this policy are communicated to all members of the trust community.