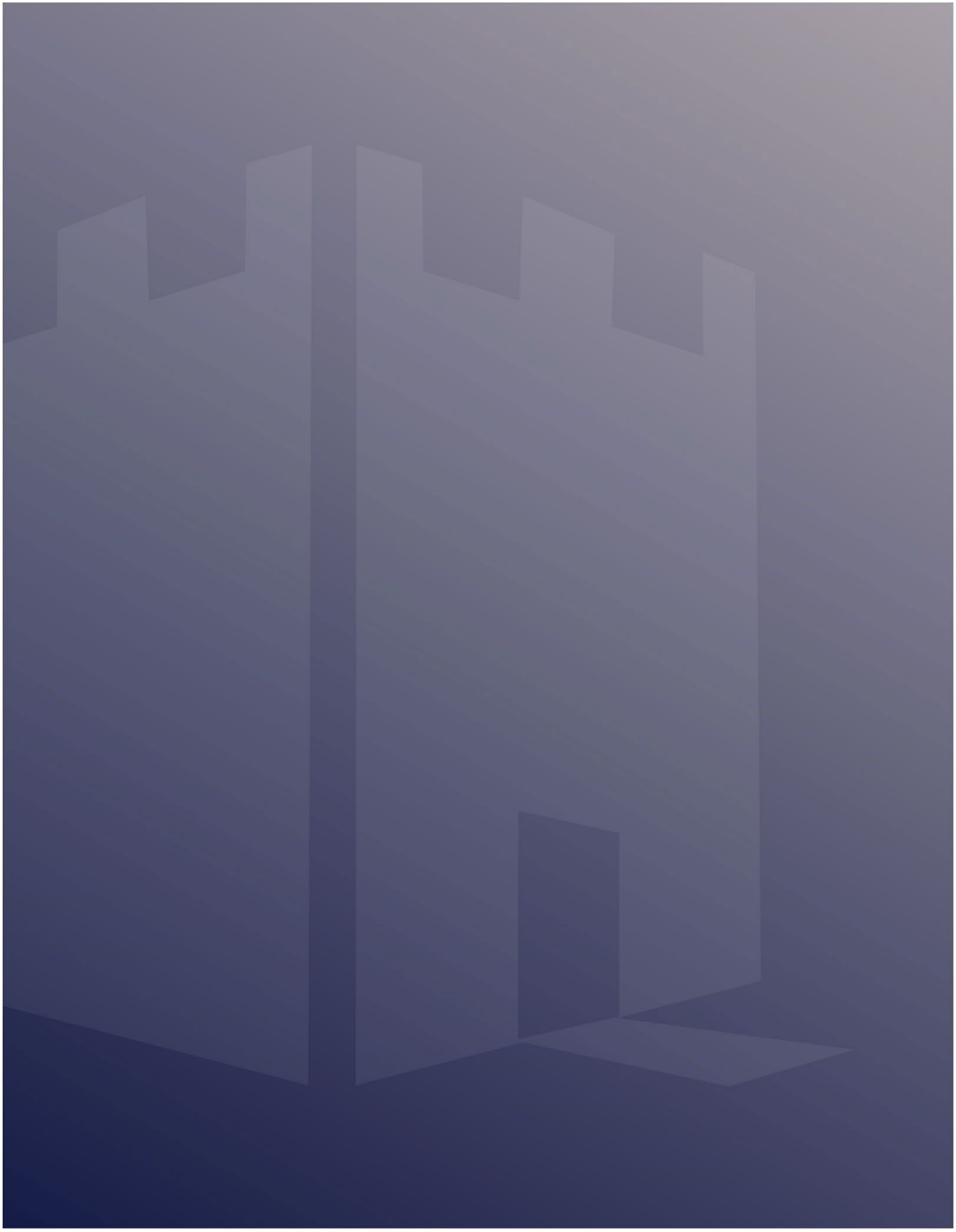
PONTEFRACT
ACADEMIES TRUST

Online Safety Policy



Summary:

The Trust has created this policy with the aim of ensuring robust processes to ensure the safe use of the internet and other digital technology devices by all pupils, staff and volunteers. Pontefract Academies Trust aims to 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. We also have established clear mechanisms to Identify, Intervene and escalate an Incident, where appropriate.

Author	Director of Inclusion & Safeguarding		
Applies to: (please check as appropriate)	Staff ☑	Pupil ☑	Community ☐
Ratifying Committee(s):	Audit & Risk Committee		
Available on:	Compliance Library ☑	Website ☐	
Date of Approval:	10/10/2025		
Date of Next Formal Review: (ensure this is aligned to committee meeting dates)	09/10/2026		
Review Period:	Annually		
Status:	Non-contractual		
Owner:	**Pontefract Academies Trust**		
Version:	2.1		

Document Control

Date	Version	Action	Amendments
August 2022	01	Policy created	
September 2023	02	Reviewed	Updated to reflect latest KCSIE guidance
September 2024	2.1	Reviewed.	Updated to reflect latest KCSIE guidance
July 2025	2.2	Reviewed	Updated to reflect latest KCSIE guidance Inclusion of AI – Generative AI use in schools as part of GDPR considerations

Contents

1. Statement of intent

Pontefract Academies Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. Online safety encompasses all devices with access to online including personal information and harmful material. Well trained staff can support pupils to access a connected world in a safe and effective way. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified with 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.
- **Contact:** being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **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 that the Trust has implemented are to protect pupils and staff which revolve around these areas of risk. The Trust has created this policy with the aim of ensuring robust processes to ensure the safe use of the internet and other digital technology devices by all pupils, staff and volunteers. Pontefract Academies Trust aims to 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. We also have established clear mechanisms to Identify, Intervene and escalate an Incident, where appropriate.

2. Legal framework

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

- Voyeurism (Offences) Act 2019 Voyeurism (Offences) Act 2019 (legislation.gov.uk)
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 Data protection: The Data Protection Act - GOV.UK (www.gov.uk)
- DfE (2021) 'Harmful online challenges and online hoaxes' Harmful online challenges and online hoaxes - GOV.UK (www.gov.uk)

- 'Keeping children safe in education 2025' Keeping children safe in education - GOV.UK (www.gov.uk)
- DfE (2019) 'Teaching online safety in school' Teaching online safety in schools - GOV.UK (www.gov.uk)
- DfE (2022) 'Searching, screening and confiscation' Searching, screening and confiscation at school - GOV.UK (www.gov.uk)
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
- UK Council for Child Internet Safety (2020) 'Education for a Connected World - 2020 edition' Education for a Connected World - GOV.UK (www.gov.uk)
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security' Small Business Guide: Cyber Security - NCSC.GOV.UK
- Generative Artificial Intelligence in Schools Generative artificial intelligence (AI) in education - GOV.UK

This policy operates in conjunction with the following Trust policies:

- Managing Allegations Policy
- Child protection and safeguarding policy
- Anti-bullying policy
- PSHE policy
- RSE and health education policy
- Searching, screening and confiscation policy
- Staff code of conduct
- Behaviour and Relationships policy
- Data protection policy
- Confidentiality policy
- Pupil remote learning policy
- Technology acceptable use agreement for pupils
- Technology acceptable use agreement for staff

3. Roles and responsibilities

The Trust Board and SPRB are responsible for:

- Providing all pupils with a safe environment in which to learn and develop as part of a broad and balanced curriculum.
- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Ensuring that there are appropriate filtering and monitoring systems in place that include the use of generative AI.
- Ensuring that all relevant Trust policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

- Ensuring their own knowledge of online safety issues is up-to-date.

The Director of Safeguarding and Inclusion Is responsible for:

- Reviewing this policy on an annual basis.
- 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 online safety is a running and interrelated theme throughout the Trust's policies and procedures, including those related to the curriculum, teacher training and safeguarding.
- Ensuring online safety practices are audited and evaluated.
- Acting as the named point of contact within the Trust on all safeguarding issues.
- Providing training so that all staff understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Ensuring that filtering and monitoring systems are appropriately reviewed and acted upon.
- Reporting to the school performance review board about online safety on a termly basis.

The Headteacher is responsible for:

- Supporting the DSL and the deputy DSL 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 and any potential risks are acted upon.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the Trust is keeping pupils safe.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Ensure that all staff receive the appropriate training in relation to online safety and that they are aware and show understanding of the school’s filtering and monitoring procedures.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and external IT provider.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a co-ordinated approach is implemented.
- Ensuring safeguarding is considered in the school'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.
  Co-ordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establish a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Support parents to understand the risks online and how to support In keeping their children safe.
- 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 school's provision.
- Ensure that members of the safeguarding team are trained to an adequate level in order to respond to filtering and monitoring alerts.

The Trust's external IT provider are responsible for:

- Providing technical support in the development and implementation of the Trust's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Trust.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate and that appropriate reports are provided to the Trust in line with the National Filtering and Monitoring Standards.
- Ensuring that risk assessments are up to date, effective and provided to the Trust when requested.
- Provide logfile Information to the Trust on a regular basis and ensure that these are Interpreted so that alerts can be prioritised for Intervention.

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.
- Attend and receive appropriate training.
- Having an awareness of online safety issues to enable them to identify signs of abuse online.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school’s reporting procedure.
- Are aware of the early help procedure and referral processes to support pupils who may be at risk of harm online.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Sharing pupil and student expectations on how to keep themselves safe and others online.
- Adhering to the Acceptable Use Agreement highlighted in the Staff Code of Conduct.

Pupils are responsible for:

- Adhering to the acceptable use of ICT and being safe online and other relevant policies such as the Behaviour and Relationship Policy which are shared as part of the curriculum, classroom expectations (Primary) referenced in student planners (Secondary).
- Seeking help from school 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.

4. 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 using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' 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 all Trust operations in the following ways:

- Staff and SPRB members receive regular training.
- External provider RM provides regular reports and monitoring lists with accompanying support and intervention.
- RM SafetyNet provides alerts of online safety risks into each safeguarding team via the DSL's in order to investigate.
- Risk assessments that provide operational procedures at all levels to ensure online safety.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Staff receive regular information through CPD and briefings on online safety and new trends.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted regularly on the topic of remaining safe online.

Handling online safety concerns

Any disclosures made by pupils 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 as part of the Child Protection and Safeguarding Policy, that pupils 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 pupils 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's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

RM SafetyNet is the preferred filtering and monitoring system and is an essential component to the Trust's approach to online safety in our settings. Its primary purpose is to create a safe and secure digital environment for students and staff while ensuring that online activities align with the school's safety policies and educational goals. Its function is to block or restrict access to inappropriate or harmful content on the internet. This includes websites with explicit, violent, or otherwise unsuitable material for pupils. Filtering and monitoring systems also include misinformation, disinformation and conspiracy theories that could cause harm. In addition to filtering, monitoring systems can track online activities of pupils and staff. This allows schools to identify and address any policy violations or safeguarding concerns promptly. Alerts are reported directly into school into the school Safeguarding Team.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Headteacher, it is reported to the Director(s) of School Improvement/ Chair of the SPRB / Director of Safeguarding, following the managing allegations policy.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and External IT provider, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour for Learning Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police. The Trust avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. 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 school's response are recorded by the DSL using CPOMS.

5. 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 trust is aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND. Pastoral support and access to disclosures is a key element of our curriculum.

Cyberbullying against pupils 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.

6. Children with SEND

The Trust is aware that children with SEND can be more at risk online. This could be down to a number of factors such as peer isolation, missed indicators of abuse or communication barriers. It is important that the DSL works closely with the SENCO to ensure that they are aware of these additional risks and are confident to support staff ensure that all pupils can use online material safely and can protect themselves from harm.

7. Child-on-child sexual abuse and harassment

Pupils 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 school, off and online, and will remain aware that pupils 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 a Trust culture that normalises abuse and leads to pupils 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 school recognises the growing risk from adult offenders using AI for sextortion and that even 'fake' images are criminal. The Trust Safeguarding procedures will be followed in such cases and educating the pupils on harms and risks to AI generated content.

The school 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 pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child Protection and Safeguarding Policy.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy and the Behaviour and Relationships Policy.

7. 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 pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil 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 pupil 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 pupil 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 pupil feel 'special', particularly if the person they are talking to is older.
- The pupil 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 pupils 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 Director of Safeguarding with the DSL's 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 school 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 to behave in sexually inappropriate ways through the internet. In some cases, a pupil 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 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 to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils 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 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 pupils at increased vulnerability to radicalisation, as outlined in the Child Protection and Safeguarding Policy under the PREVENT duty. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised. All staff will have access to training that covers the Prevent Duty and the Channel Program.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy.

8. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, due to attempting to create an online community to seek acceptance. Trends such as social influencers can create an unrealistic sense of identity which can in turn lead pupils to question themselves and have a negative impact on self-esteem.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil'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 pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Child Protection and Safeguarding Policy.

9. 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 pupil 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 pupils in the school, 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 pupils, and whether the risk is one that is localised to the school 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 Director of Safeguarding and / or 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 Headteacher 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 pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.

- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' 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 pupils at risk of harm, e.g. it encourages children 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 pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible in consultation with the Trust.

10. 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 Trust will factor into its approach to online safety the risk that pupils 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 pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to outside agencies such as Early Help or to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils 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 Trust-owned devices or on Trust networks through the use of appropriate firewalls.

11. 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 pupils 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.

Information about the Trust's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, Behaviour and Relationships Policy and the Child Protection and Safeguarding Policy.

12. Online safety and curriculum

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

- ICT
- PSHE

Online safety teaching is always appropriate to pupils' ages and developmental stages.
Pupils 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 pupils 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.
- 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 pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in **Appendix A** of this policy.

The DSL is involved with the development and review of the Trust's online safety curriculum. Pupils 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 Trust recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

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

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. 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 pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.
Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils 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 pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils 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 pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil 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.

13. Use of technology in the classroom

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

- Laptops
- Tablets
- Desktop computers

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

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

14. Use of smart technology

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

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the Trust's Technology Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the Trust's Staff Code of Conduct and Acceptable Usage Policy.

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

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.

Pupils will not be permitted to use smart devices or any other personal technology during the school day. In primary school settings these will be held safely and securely if there is not an option to leave a device at home, in secondary setting the expectation will be that these will not be in sight during school hours. Should mobile devices be found to be being used the Behaviour and Relationships Policy will be applied.

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

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

15. Educating parents

The Trust works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the Trust's approach to online safety and their role in protecting their children new starter information and newsletters / parent workshops. Information on sanctions regarding inappropriate use is included within the Trust Behaviour and Relationships Policy.
Parents 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 pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents 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.

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

- Parents' evenings.
- Training sessions.
- Newsletter.
- Online resources.

17. Filtering and monitoring online activity

The Trust Board ensures the Trust's ICT network has appropriate filters and monitoring systems in place. The Trust Board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Headteacher and external IT providers undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the Trust implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. The external IT provider undertakes weekly checks on the filtering and monitoring systems to ensure they are effective and appropriate. Reports are generated and shared with the Headteachers, DSL's and Director of Safeguarding in order to assess trends and swiftly instigate intervention if required.

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

Deliberate breaches of the filtering system are reported to the Headteacher, DSL and the external IT provider, who will escalate the matter appropriately. If a pupil 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 Staff Code of Conduct.

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 Trust's network and Trust-owned devices are appropriately monitored. All users of the network and Trust-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 the external IT provider. Firewalls are switched on at all times. The external IT provider review the firewalls on a weekly basis 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 the external IT provider.

All members of staff have their own unique usernames and private passwords to access the Trust's systems. Pupils in key stage three and above are provided with 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 the external IT provider 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 Headteacher 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.
Full details of the Trust's network security measures can be found in the Information Policy.

19. The Use of Generative Artificial Intelligence.

As part of our commitment to online safety and compliance with data protection legislation, the Trust recognises the growing use of generative Artificial Intelligence (AI) tools in educational and administrative contexts. While these technologies offer significant potential to enhance learning and efficiency, they must be used responsibly and in line with data protection laws, including the UK General Data Protection Regulation (UK GDPR).

Staff must not input, share, or process any personal or identifiable information (such as full names, addresses, dates of birth, student records, or any data that could directly or indirectly identify an individual) into any generative AI platform, unless the platform has been formally assessed, approved, and secured under the Trust's Data Protection and IT Security policies.

Sharing identifiable data with third-party AI systems may constitute a breach of UK GDPR, and may expose individuals to risk and the Trust to legal liability. Staff are reminded that all data shared must adhere to the principles of data minimisation, purpose limitation, and security.

Any misuse of generative AI in relation to personal data will be treated as a serious breach of the Trust's Data Protection and Online Safety Policies and may result in disciplinary action.

This policy will be reviewed regularly to reflect technological advances and evolving legal guidance on AI and data protection.

19. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Trust Code of Conduct.

Staff given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement / Code of Conduct. Personal email accounts are not permitted to be used on the school site. Any email that contains sensitive or personal information is only sent using secure and encrypted email or password protected.

Staff members and pupils are required to block spam and junk mail, and report the matter to the external IT provider. The Trust's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Any cyber-attacks initiated through emails are managed in line with the Information Policy.

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 members are advised that their conduct on social media can have an impact on their role and reputation within the Trust. 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 receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and Headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils 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 school community on social media are reported to the DSL 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 school

The use of social media on behalf of the school is conducted in line with the Trust Social Media Policy. The Trust's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the Headteacher to access to the Trust's social media accounts.

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

21. The school website

The Headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The Headteacher will ensure that they liaise with the Trust's Marketing and Communication Manager to ensure that all content on the school website is up to date.

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 by the Marketing and Communications Manager and are in line with Trust policy.

22. Use of devices

Trust-owned devices

Staff members may be issued with some or all of following devices to assist with their work:

- Laptop
- Mobile phone
- Tablet
- Surface Book Pro

Pupils 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 Trust Code of Conduct. Staff and pupils are not permitted to connect Trust-owned devices to public Wi-Fi networks. All Trust-owned devices are password protected. All mobile Trust-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen. 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.

The external IT provider review all Trust-owned devices on a monthly 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 the external IT provider.

Cases of staff members or pupils found to be misusing Trust-owned devices will be managed in line with the Code of Conduct and Behaviour Policy respectively.

Personal devices

Personal devices are used in accordance with the Code of Conduct. Any personal electronic device that is brought into school is the responsibility of the user. Pupils are not permitted to use personal devices during the school day without consent and supervision from a member of staff.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations Policy. 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 Headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

Pupils are not permitted to use their personal devices during lesson time or when moving between lessons. If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office or in student services.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil 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 and as part of a One Page Profile / My Support Plan / EHCP.

Pupils' devices can be searched, screened and confiscated in accordance with the Trust Behaviour and Relationships Policy. If a staff member reasonably believes a pupil'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.

Appropriate information is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

23. Remote learning

All remote learning is delivered in line with the Trust's Pupil Remote Learning Policy.

The Trust will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The Trust will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The Trust will ensure that all Trust-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The Trust will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the Trust.

24. Monitoring and review

The Trust recognises that the online world is constantly changing; therefore, the DSL, the external IT provider and the Headteacher conduct **half-termly** light-touch reviews of this policy to evaluate its effectiveness.

The Trust Board, Executive Directors and Director of Safeguarding review this policy in full on an **annual** basis and following any online safety incidents.

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

Appendix A – Online harms and risks (curriculum coverage)

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	Health education Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	**Primary school** - Relationships education **Secondary school** - RSHE Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	**Primary schools** Relationships and health education **KS2 and above** Computing **Secondary schools** RSHE Citizenship

Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails	**Primary schools** Relationships education **Secondary schools**
	• The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support	RSHE Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	**Primary schools** Relationships education **Secondary schools** RSHE Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	**Primary schools** Relationships education **Secondary schools** RSHE Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	**Primary schools** Relationships education **Secondary schools** RSHE Computing

Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	Health education Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	**Primary schools** Relationships education
		Secondary schools RSHE Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	**Primary schools** Relationships education **Secondary schools** RSHE Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	**Primary schools** Relationships education **Secondary schools** RSHE Computing **KS4** Citizenship

Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	**Primary schools** Relationships education **Secondary schools** RSHE
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence	**Primary schools** Relationships education **Secondary schools** RSHE
	• How and where to get help if they are worried about involvement in violence	
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	**Primary schools** Relationships education **Secondary schools** RSHE Computing

Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	**Primary schools** Relationships education **Secondary schools** RSHE
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	**Secondary schools** RSHE
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following:	**Secondary school:**

	• That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	RSHE

Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	**Primary schools** Relationships education **Secondary schools** RSHE Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	**Secondary schools** RSHE

Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues	Health education
	• That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	**Primary schools** Relationships education **Secondary schools** RSHE
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	**Secondary schools** RSHE
Suicide, self harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	