THE EDUCATION VILLAGE ACADEMY TRUST

On Line Safety Policy

EVAT Version Control Document

Version:	Date:	Policy Owner:	Amendments made by:	Details of amendments made:	Reviewed by:	Approved by:
V0.1	March 23	Marie Roe	Marie Roe	Draft policy & incorporation of feedback from ELT	ELT	
V1.0	March 23	Marie Roe	Wendy Turpin	Final Version	ELT	27/042023

Monitoring and review

This policy is reviewed every **two years** by the Policy Owner: Marie Roe

The scheduled review date for this policy is **April 2025**.

Values and Ethos

Our values and ethos are inclusive and child centred. Our Trust is founded on the principles of inclusivity, diversity and fairness, and they are fundamental to our delivery of exceptional learning experiences.

EVAT stands for:

- **E**xcellence and high standards
  - a can-do culture and no-excuses ethos
- **V**alues driven with a deep sense of purpose
  - putting children and young people first
  - behaving ethically
- **A**mbition and aspiration for all
  - irrespective of background or barriers – being truly inclusive
- **T**eamwork
  - we do more, better and faster, together

We are a village. We collaborate, with our learners, their families and our communities, to provide exceptional education so that all the children and young people we serve achieve the best possible outcomes.

Our Ethos is to:

- Create a nurturing and friendly atmosphere and provide an environment where everyone feels valued for who they are
- Bring out the best in every child and young person and meet the full range of their individual needs
- Provide different and unique experiences, challenges and activities
- Show tolerance and respect for each other
- Prepare our children and young people for lifelong learning
- Improve the life chances of every child and young person we serve.

This policy, and its associated procedures and protocols, are based on these key principles.

Table of Contents

Statement of intent

The Education Village Academy Trust (EVAT) understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the Trust; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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
- **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 implemented to protect pupils 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 by all pupils and staff.

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 (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- 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'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following Trust/school policies:

- Social Media Policy
- Managing Allegations of Abuse Against Staff and Volunteers Policy
- ICT and Electronic Device (Acceptable Use) Policy
- Cyber Security Strategy and Incident Response Plan
- Safeguarding and Child Protection Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- GDPR Data Protection Policy
- Photography and Images Policy (Appendix 3 of Safeguarding)
- Protecting Children from Extremism and Radicalisation Policy
- Remote Education Policy

Roles and responsibilities

The Board of Trustees is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance
- Ensuring the Designated Safeguarding Lead's (DSL) remit covers online safety
- 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 and at regular intervals
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that all relevant Trust and school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them

The Executive Leadership Team is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the Trust's (and its schools') policies and procedures, including in those related to the curriculum, teacher training and safeguarding
- 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
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe
- Working with the DSL and RM technicians to conduct termly light-touch reviews of this policy

- Working with the DSL, the Chief Operating Officer and the Board of Trustees to update this policy on an annual basis

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCo and RM technicians
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented
- Ensuring safeguarding is considered in the school's approach to remote learning
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure
- 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, and using this data to update the school's procedures
- Reporting to governing bodies about online safety on a termly basis
- Working with the Principal and RM technicians to conduct a termly light-touch reviews of this policy
- Working with the Chief Operating Officer and the Board of Trustees to update this policy on an annual basis

RM technicians 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 Chief Operating Officer
- Ensuring that the school's filtering and monitoring systems are updated as appropriate
- Working with the DSL, Principals and Chief Operating Officer to conduct termly light-touch reviews of this policy

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 pupils may be unsafe online

- Reporting concerns in line with the school's reporting procedure
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies
- 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

Managing online safety

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 individual school'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 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 the Trust's operations in the following ways:

- Staff, Educational Standards Committee (ESC) members, and Trustees 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 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 Trust's Safeguarding and Child Protection Policy.

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 – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

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. If the concern is about the Principal or Executive Principal, it is reported to the Chief Executive.

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

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

The school 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 Safeguarding and Child Protection Policy.

All online safety incidents and the school's response are recorded by the DSL.

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 will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

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.

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 school and 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 and Trust 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-on-child Abuse Policy and the Social Media Policy.

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

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, e.g. 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 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 online
- 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 Safeguarding and Child Protection 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 Trust's Protecting Children from Extremism and Radicalisation Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

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 Trust's Protecting Children from Extremism and Radicalisation Policy.

Mental health

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 individual school's approach to Social, Emotional and Mental Health (SEMH).

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 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 Safeguarding and Child Protection Policy

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, 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 individual pupils at risk where appropriate.

The DSL and Principal 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.

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 and its schools will factor into their 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 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 Principal will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

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.

Online safety and the curriculum

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

- RSHE (secondary schools)
- Relationships and health education (primary schools)
- PSHE
- Citizenship
- ICT

Online safety teaching should always be 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
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The risks pupils may face online are considered when developing the curriculum. DfE guidance on the online risks that should be included in the curriculum is included at Appendix A of this policy.

The DSL will be involved with the development of the school'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.

Relevant members of staff, e.g. the SENDCo and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school 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 will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Principal and DSL will 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 will 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 will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be 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 will ensure 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 Safeguarding and Child Protection 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 Safeguarding and Child Protection Policy.

Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- Intranet/RM Unify
- Email
- Cameras

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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

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

Use of smart technology

While the Trust and its schools recognise that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school 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 ICT and Electronic Devices Policy.

The Trust and its schools recognise 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 whilst in the classroom, unless it is relevant to the content of the lesson or the curriculum. Teachers will advise/direct pupils when it is permitted for them to use smart devices or other personal technology.

Where it is deemed necessary, the Trust will ban a pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

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 its schools are kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (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.

Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year 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 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 will be raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- The school's website and online resources

Internet access

Pupils, staff and other members of the school community will only be granted access to the Trust's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access by RM.

All members of the school community will be encouraged to use the Trust'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.

Filtering and monitoring online activity

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

The Chief Operating Officer and RM technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be 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. RM technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Chief Operating Officer. Prior to making any changes to the filtering system, RM technicians, the Chief Operating Officer and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by RM technicians. Reports of inappropriate websites or materials will be made to the RM technician(s) immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and RM technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the school's Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Trust's 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 Trust's network and Trust-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Safeguarding and Child Protection Policy.

Network security

Technical security features, such as anti-virus software, will be kept up to date and managed by RM technicians. Firewalls will be switched on at all times. RM technicians will review anti-virus software on a weekly basis. Firewalls are reviewed on a termly basis to ensure they are running correctly, and to carry out any required updates.

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

All members of staff, Trustees and Educational Standard Committee members will have their own unique usernames and private passwords to access the school's systems. Pupils in secondary education (Key Stage 3 onwards) will be provided with their own unique username and private passwords. A limited number of primary aged children (Key Stage 2) also have a unique username and password.

Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords of a suitable length and complexity are set by users to ensure they remain secure.

With the introduction of RM Unify, staff members are able to reset their own passwords. However, users can inform RM technicians if they forget their login details, who will arrange for the user to access the systems under different login details if necessary. Users will not be permitted to share their login details with others and will not be 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 will be informed and will decide the necessary action to take.

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

Full details of the Trust's network security measures are set out in the Trust's Cyber Security Strategy and Incident Response Plan.

Emails

Access to and the use of emails will be managed in line with the Trust's GDPR Policy and the ICT and Electronic Device (Acceptable Use) Policy.

Staff and pupils will be given approved Trust email accounts and will only be 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 and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report any suspicious spam and junk mail to RM technicians. The Trust's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. An annual assembly will be undertaken where a phishing email and other malicious emails will be described – this assembly will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Trust's Cyber Security Strategy and Incident Response Plan.

Social networking

The use of social media by staff and pupils will be managed in line with the Trust's Social Media Policy.

The school website

The Principal will work with the Chief Operating Officer to ensure the overall content of the school website is appropriate, accurate, up-to-date and meets government requirements.

The website will be managed in line with the Trust Website Policy.

Use of devices

Staff members and pupils will be issued with Trust-owned devices to assist with their work, where necessary. Requirements around the use of Trust-owned devices can be found in the Trust's ICT and Electronic Device (Acceptable Use) Policy.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Trust's ICT and Electronic Devices Policy and Pupils' Personal Electronic Devices Policy.

Remote learning

All remote learning will be delivered in line with the Trust's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

Monitoring and review

The Trust recognises that the online world is constantly changing; therefore, the DSL, RM technicians and the Chief Operating Officer will conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The Board of Trustees will review this policy on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is April 2024.

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

Public Sector Equality Duty

In preparing this policy, the author has given due regard to the Public Sector Equality Duty; that is, they have considered any potential impact on people who share certain protected characteristics. The relevant protected characteristics are age, disability, gender reassignment, race, religion or belief, marriage and civil partnership, sex and sexual orientation.

Appendices:

Appendix A: DfE Guidance on online risks for inclusion in the curriculum

Appendix A: DfE Guidance on online risks for inclusion in the curriculum

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 will include 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	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include 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)	This risk or harm will be covered in the following curriculum areas: • Primary schools - Relationships education • Secondary schools - RSHE • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• 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 Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • 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 education • Secondary schools - RSHE • KS2 and above Computing • KS3 and KS4 - 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 will include the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • 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	This risk or harm will be covered in the following curriculum areas: • Primary schools - Relationships education • Secondary schools- RSHE • Computing

	• Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	This risk or harm will be covered in the following curriculum areas: • 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 will include the following:	This risk or harm will be covered in the following curriculum areas: • Primary schools -

	• 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	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 will include 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	This risk or harm will be covered in the following curriculum areas: • 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 will include 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 to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: • 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 will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: • 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 will include 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	This risk or harm will be covered in the following curriculum areas: • 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 will include 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	This risk or harm will be covered in the following curriculum areas: • Primary schools - Relationships education • Secondary schools - RSHE • Computing

	• The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	• Key Stage 4 - Citizenship
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include 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	This risk or harm will be covered in the following curriculum areas: • Primary schools - Relationships education • Secondary schools - RSHE
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into	This risk or harm will be covered in the

	offline violence. Teaching will include 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 • How and where to get help if they are worried about involvement in violence	following curriculum areas: • Primary schools - Relationships education • Secondary schools - RSHE
Fake profiles	Not everyone online is who they say they are. Teaching will include 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	This risk or harm will be covered in the following curriculum areas: • 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, gangs and financial exploitation. Teaching will include 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	This risk or harm will be covered in the following curriculum areas: • Primary schools - Relationships education • Secondary schools - RSHE

	never the fault of the child who is abused and why victim blaming is always wrong.	
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 will include the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • 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 • 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	This risk or harm will be covered in the following curriculum areas: • Secondary schools - RSHE
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following: • 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, e.g. revenge porn or people trafficked into sex work	This risk or harm will be covered in the following curriculum areas: • Secondary Schools - RSHE

Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include 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	This risk or harm will be covered in the following curriculum areas: • 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 will include 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 • That 'easy money' lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm will be covered in the following curriculum areas: • Secondary schools - RSHE
Impact on quality of life, physical and mental health	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	This risk or harm will be covered in the following curriculum areas:

and relationships	online and offline. Teaching will include 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 • 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	• Health education
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: • Primary schools - Relationships education • Secondary schools - RSHE

Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: • Strategies for positive use • How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: • 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.	