MARK Education Trust

Online Safety Policy

Policy document provenance

Approver:	Trust board
Date of approval:	March 2026
Reviewer:	Safeguarding & IT Link trustees
Policy owner:	Head of IT
Policy author(s):	Head of IT with Safeguarding Leads
Date of next review:	March 2027

Version Control:	V1.0 March 2026
	V1.1
Summary of key changes made since last review:	Updated to apply across all schools in the trust in both settings. Updated to ensure KCSIE requirements are met. Further updates might be required when KCSIE 2026 is published in September 2026. Formatting updates to bring in line with the trust's policy template.

Unless there are legislative or regulatory changes in the interim, this policy will be reviewed on an annual basis. Should no substantive changes be required at this point, the policy will move to the next review cycle.

Related policies:	MARK Education Trust Child Protection and Safeguarding Policy MARK Education Trust Acceptable Use Agreement for students/pupils and staff MARK Education Trust Data protection policy MARK Education Trust Cyber Security Policy MARK Education Trust Behaviour Policy MARK Education Trust Mobile Phone Policy MARK Education Trust Staff Disciplinary Policy and Procedures MARK Education Trust Staff Code of Conduct Anti-Bullying Policy in each school Relationships, Sexual Education and Health Education Policy (RHSE) in each school

Contents

1. Statement of intent

MARK Education Trust understands that using online services is an important aspect of raising educational standards, promoting student 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 students/pupils and staff.

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

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising, phishing, financial scams along with sextortion and adults posing as children or young adults.
- **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 students/pupils and staff revolve around these areas of risk.

This policy has been developed with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students/pupils and staff through the trust systems, as well as any devices that are provided.

2. Legal framework

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

- Meeting digital and technology standards in schools and colleges 2023
- Teaching Online Safety in Schools January 2023
- 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 (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2025) 'Keeping children safe in education 2025'
- Department for Digital, Culture, Media and Sport UK Council for Internet Safety (2020)'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2018) 'Searching screening and confiscation'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security' UK Council for Child Internet Safety (2020) 'Education for a Connected World– 2020 edition'
- DfE (2023) 'Generative artificial intelligence in education'
- Counter - Terrorism and Security Act 2015
- Online Safety Act (2023), now fully in force, which introduces statutory expectations on online platforms and informs KCSIE 2025 compliance.

3. Roles and responsibilities

3.1 The board of trustees is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance
- Approving this policy on an annual basis
- Ensuring the board's own knowledge of online safety issues is up to date including about filtering and monitoring, risk assessments and the trust's online safety strategy
- Have oversight for the trust's filtering and monitoring arrangements
- Ensuring that all relevant trust policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

3.2 The headteacher in each school is responsible for:

- Ensuring the Designated Safeguarding Lead's (DSL) remit covers online safety
- Ensuring that all relevant local school level policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training
- Ensuring online safety practices are audited and evaluated
- Ensuring that there are appropriate filtering and monitoring systems in place
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students/pupils can develop an appropriate understanding of online safety
- Organising engagement with parents and carers to keep them up to date with current online safety issues and how the trust is keeping students/pupils safe
- Working with the DSL and IT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and the head of IT to update this policy on an annual basis.

3.3 The DSL in each school is responsible for:

- Taking the lead responsibility for online safety in the school- including filtering and monitoring
- Acting as the named point of contact within the school on all online safeguarding issues
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students/pupils with SEND face online
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.

- Liaising with the trust's HR team to ensure that all staff undergo safeguarding and child protection training, including online safety, at induction to Level 1 Standard
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO and IT technicians
- Ensuring online safety is recognised as part of the trust's safeguarding responsibilities, that a coordinated approach is implemented and incidents are recorded via My Concern in a timely way
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Ensuring appropriate referrals are made to external agencies, as required
- Keeping up to date with current research, legislation and online trends including Generative AI tools and services
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students/pupils and staff
- Ensuring all members of the school community understand the reporting procedures
- 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 trust's procedures
- Reporting to the local governing committee about online safety alongside the safeguarding report on a termly basis
- Working with the headteacher and the head of IT to conduct reviews of this policy.

3.4 IT 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 headteacher
- Ensuring that the trust's filtering and monitoring systems are updated, installed where required and configured as appropriate
- Working with the DSL, the head of IT and headteacher to conduct half-termly light-touch reviews of this policy.

3.5 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 students/pupils may be unsafe online.

- Reporting concerns in line with the trust's reporting procedures
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum
- When the trust hires out its facilities e.g. hall and sports areas, it has a responsibility to keep children safe.

3.6 Students are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies
- Seeking help from staff if they are concerned about something they or a peer have experienced online
- Reporting online safety incidents and concerns in line with the procedures within this policy.

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.

Each school's 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 students/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 school operations in the following ways:

- Staff and governors receive regular training via Inset days and weekly updates
- 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 regularly on the topic of remaining safe online

5. The curriculum

Online safety is embedded throughout the curriculum. The trust's approach to online safety curriculum is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in trust' guidance.

Students and 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.

Online safety teaching is always appropriate to students/pupils' ages and developmental stages.

This will include things such as awareness of media literacy, critical evaluation of digital content, digital footprints and their lasting impact, privacy, data, and cyber security, copyright and plagiarism and the responsible use and risks of generative AI Literacy.

The risks students/pupils may face online are always considered when developing the curriculum. Students/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 DSL and the Online Lead in each school are involved with the development of the online safety curriculum.

The trust recognises that, while any student can be vulnerable online, there are some students/pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students/pupils with SEND and LAC. Relevant members of staff, e.g. the SENDCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these students/pupils receive the information and support they need, and in response to instances of harmful online behaviour from students/pupils.

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

External visitors may be invited into trust 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 trust 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 students/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 student/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 student/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 students/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 students/pupils disclose or raise during online safety lessons and activities, they will report this to the DSL in line with the trust's child protection and safeguarding policy.

6. Staff training

All new staff joining the trust receive safeguarding and child protection training, which includes online safety training, during their induction. The training will cover how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems.

Online safety training for all staff is updated annually and is delivered in line with advice from local safeguarding partners with ongoing and regular online safety updates via staff forums. Training covers AI risks, misinformation/disinformation and the school's duties under the Online Safety Act.

All those that govern in the trust, are required to complete annual safeguarding training as required in KCSIE.

7. Educating parents and carers

Each school works in partnership with its parents and carers to ensure its students/pupils stay safe online in school and at home through the newsletter and regular bulletins.

Parents and carers can seek further guidance on keeping children safe online from the GOV.UK trusted site [Help your child stay safe online - Kids Online Safety]

8. Remote learning for students/pupils

Remote learning for students / pupils is only accessed in very specific circumstances and is agreed on a case-by-case basis. When deemed to be appropriate, it is delivered with specific consideration of additional online risks during remote education (as highlighted in KCSIE) as set out in this policy and the trust's child protection and safeguarding policy

9. Internet access

Students, staff and other members of the trust community are only 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 the ICT department.

10. Filtering and monitoring online activity

The Head of IT, headteachers and DSL's ensure the trust's ICT network has appropriate filters and monitoring systems in place, including for AI generated content, and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The trust will use the DfE Plan Technology for Your School self-assessment tool annually to review the effectiveness and appropriateness of filtering and monitoring systems.

The Head of IT undertakes a risk assessment to determine what filtering and monitoring systems are required, and IT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

The filtering and monitoring systems the school implements will be appropriate to students/pupils' ages, the number of students/pupils using the network, how often students/pupils access the network, and the proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system are directed to the Head of IT who will conduct a Risk Assessment with the DSL, prior to the IT technicians making any changes.

Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and IT technicians, who will escalate the matter appropriately.

If a student has deliberately breached the filtering system, they will be disciplined in line with the student acceptable use policy and behaviour policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the staff acceptable use policy and staff disciplinary 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 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 will manage the situation in line with this policy and the trust's child protection and safeguarding policy.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

11. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the Head of IT and IT technicians, in line with the trust's cyber security policy. The trust is working towards meeting the DfE's National Cyber Security Standards for Schools (NCSC).

Firewalls are switched on at all times, IT technicians review the firewalls on a termly basis to ensure they are running correctly, and to carry out any required updates.

Staff and students/pupils are not to download unapproved software or open unfamiliar email attachments, and staff undertake annual National Cyber Security Centre (NCSC) training.

Staff and students/pupils report all malware and virus attacks to IT technicians.

All staff and students/pupils have their own unique usernames and private passwords to access the trust's systems. Staff and students/pupils are responsible for keeping their passwords private. Users must inform IT technicians if they forget their login details. The ICT support team will reset passwords and/or remind them of their username if required.

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 cyber security policy.

12. Emails

Access to and the use of emails is managed in line with the trust's data protection policy and acceptable use agreement.

Staff and students/pupils are given approved school email accounts and are only able to use these accounts at the trust and when doing school-related work outside of school hours or when off the school site.

Prior to being authorised to use the email system, staff and students/pupils must agree to the acceptable use agreement.

The trust's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students/pupils are made aware of this.

Chain letters, spam and all other emails from unknown sources are deleted automatically by the trust's filtering systems.

Staff and students/pupils are required to block spam and junk mail and report any concerns about worrying spam and junk mail that arrive despite our filtering systems.

The ICT team will send regular emails where they explain what a phishing email and other malicious emails might look like – this includes 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 cyber response plan.

13. Social networking

The use of social media, for personal use, by staff and students/pupils will be managed in line with the trust's staff code of conduct and acceptable use policy.

Access to social networking sites is filtered as appropriate.

Staff and students/pupils are not permitted to use social media at any time whilst on the premises of the trust. Only designated staff are able to access social media sites at school for the purpose of updating/posting.

All staff are advised that their conduct on social media can have an impact on their role and reputation within the trust and the wider community.

All staff receive annual training on how to use social media safely and responsibly.

Staff are not permitted to communicate with students/pupils or parents and carers over social networking sites and are reminded to alter their privacy settings to ensure students/pupils and parents and carers are not able to contact them on social media. This is particularly important for staff who are also parents.

Students 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 trust community on social media are reported to the headteacher and managed in accordance with the relevant policy, e.g. anti-bullying policy, staff code of conduct and behaviour policy.

13.1 Use on behalf of the trust

The trust's official social media channels are only used for official educational or engagement purposes.

Only relevant staff members are authorised by the trust 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.

14. Trust and school websites

The trust's Head of Operations is responsible for managing the content of the trust website and will ensure it is appropriate, accurate, up-to-date and meets statutory requirements. They will collaborate each school's headteacher and the marketing team to oversee the content of each school website.

All websites must comply with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and students/pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the GDPR privacy statement for students have been met.

15. Use of smart technology

While the trust recognises that the use of smart technology (including smart watches, encrypted messaging apps and emerging new devices) can have educational benefits, there are also a variety of associated risks which the trust will ensure it manages.

Students/pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the trusts' acceptable use agreement for students.

The trust has adopted a never seen, used or heard approach to the use of mobile phones for students/pupils during the school day as set out in the mobile phone policy.

Staff will use all smart technology and personal technology in line with the school's staff acceptable use agreement.

The trust recognises that students/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 school's acceptable use of ICT agreement for students/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.

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

Each 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.

Each school will consider the 4Cs (content, contact, conduct and commerce) when educating students/pupils and pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

16. Use of trust-owned devices

Staff and students/pupils are provided with trust-owned devices as necessary to assist with their work or in the delivery of the curriculum, e.g. tablets to use during lessons.

Trust-owned devices are used in accordance with the acceptable use policy.

All trust-owned devices are fitted with software to ensure they can be remotely accessed and monitored in case data on the device needs to be protected, retrieved or erased.

No software, apps or other programmes can be downloaded onto a device without authorisation from IT technicians.

Cases of staff members or students/pupils found to be misusing trust-owned devices will be managed in line with the trust's staff disciplinary procedure and behaviour policy respectively.

17. Use of personal devices

Staff personal devices are used in accordance with acceptable use agreement.

The usage of student's personal devices falls under the trust's mobile policy and behaviour policy.

Any personal electronic device that is brought into trust is the responsibility of the user.

Staff members are not permitted to use their personal devices to take photos or videos of students/pupils. The exception to this would be when a member of staff is on a school trip. In these circumstances any photos taken on personal devices should be deleted as soon as they have been uploaded to a trust approved storage.

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 as applicable.

Where a student uses accessibility features on a personal device to help them access education, or for a medical reason e.g. where a student 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.

Any concerns about visitors' use of personal devices on the trust premises are reported to the school DSL.

18. Managing reports of online safety incidents

Concerns regarding a staff member's online behaviour must be reported to the headteacher who decides on the best course of action in line with the relevant policies, e.g. staff code of conduct.

If the concern is about the headteacher, this must be reported to the CEO.

Concerns regarding a student's online behaviour are reported to the DSL in the school who investigates concerns with relevant staff members, e.g. the headteacher and IT technicians, and are dealt with in accordance with relevant policies depending on their nature, e.g. the trust's behaviour policy and child protection and safeguarding policy.

Where there is a concern that illegal activity has taken place, the headteacher will contact the police.

The school avoids unnecessarily criminalising students/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 student 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 trust's child protection and safeguarding policy.

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

19. Responding to specific online safety concerns

Any reports made by students/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 child protection and safeguarding policy.

19.1 Cyber-crime

If there are any concerns about a student/pupil that may have the skill, or interest, in computing and technology and who may have inadvertently, or deliberately, stray into cyber dependent crime, advice will be taken from the police or from Cyber Choices programme (National Crime Agency).

Each school will factor into its approach to online safety the risk that students/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 student/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 headteacher will ensure that students/pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

19.2 Online hoaxes and harmful online challenges

The DSL in each school will ensure that students/pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content, in line with this policy and with the trust's child protection and safeguarding policy.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students/pupils in the trust, they will report this to the DSL's in line with the trust's child protection and safeguarding policy

19.3 Child on Child online sexual violence and sexual harassment (KCSIE September 2025)

All concerns relating to sexual violence and sexual harassment will be reported to the DSL in school in line with the trust's child protection and safeguarding policy, the anti-bullying policy and the behaviour policy.

19.4 Youth produced sexual imagery (sharing nudes and semi nudes)

All concerns relating to youth produced imagery should be treated as a safeguarding issue and will be reported to the DSL in school in line with the trust's child protection and safeguarding policy.

19.5 Grooming and exploitation

All concerns relating to online child sexual abuse grooming and exploitation should be treated as a safeguarding issue and will be dealt with by the DSL in the school in line with the trust's child protection and safeguarding policy.

19.6 Child sexual exploitation (CSE), child criminal exploitation (CCE) and county lines

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.

Where staff have any concerns about students/pupils with relation to CSE or CCE, these will be reported to the DSL, who will manage the situation in line with the trust's child protection and safeguarding policy.

Each school will implement preventative approaches for online sexual abuse and exploitation via a range of age and ability appropriate education for students/pupils.

19.7 Indecent images of children (IIOC)

Each school will ensure that all students/pupils and staff are aware of the possible consequences of accessing indecent images of children. (IIOC)

Each school will respond to concerns regarding IIOC on its equipment and will seek to prevent accidental access to IIOC by using an internet service provider which implements filtering, firewalls and anti-spam software. If there are concerns that a criminal offence has been committed, the DSL will obtain advice from the police.

If made aware of IIOC, the DSL will act in accordance with the trust's child protection and safeguarding policy.

19.8 Cyberbullying

The trust does not tolerate cyberbullying or any kind of bullying. Please refer to the anti-bullying policy for further responses to cyberbullying.

19.9 Use of Generative artificial intelligence (AI)

The trust will take steps to prepare students/pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to student/pupils' age.

The trust will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The trust will ensure that student/pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The trust will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The trust will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

19.10 Online Hate

Online hate will not be tolerated by the trust and will be dealt with by the trust's anti -bullying and behaviour policy.

19.11 Radicalisation

If a member of staff is concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with the trust's child protection and safeguarding policy.

If a member of staff is concerned that another member of staff may be at risk of radicalisation online, the headteacher will be informed immediately and action will be taken in line with the trust's child protection and safeguarding policy.

19.12 Disinformation, misinformation, deep fakes, fake news & conspiracy theories (KCSIE 2025)

Each school will take reasonable steps to promote awareness of misinformation, disinformation, deep fakes and fake news to students/pupils, by building media literacy skills into the curriculum. This will support students/pupils to keep safe online by developing critical thinking skills, giving them the tools to spot harmful content and know how to get support, so that students/pupils can learn to assess information and sources

The DSL in each school will ensure that students/pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content, in line with section on the curriculum of this policy.

If staff have concerns that a child or parent/carer may be at risk of harm from online misinformation, disinformation, fake news, deep fakes or conspiracy theories, the DSL will be informed immediately, and action will be taken in line with the trust's child protection and safeguarding policy.

If staff are concerned about another member of staff who may be at risk of harm from online misinformation, disinformation, fake news, deep fakes or conspiracy theories, the headteacher will be informed immediately and action will be taken in line with the trust's child protection and safeguarding policy.

The police will be contacted if a criminal offence is suspected.

20. Monitoring and review

The trust recognises that the online world is constantly changing, therefore, the headteacher, the DSL of each school, Online Lead and Head of IT will review this policy at least annually to evaluate its effectiveness and will ensure it is aligned with the latest Keeping Children Safe in Education (KCSIE) guidance.

This will include each school monitoring the impact of the policy using:

- Logs of reported incidents
- Logs of internet activity (including sites visited)
- Internal monitoring data for network activity

All feedback will be collated by the Head of IT who will ensure the policy is adapted as required.

The next scheduled review date for this policy is March 2027 which will then require board approval.

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