HCAT

Online Safety Policy

EDUCATE. EMPOWER. INSPIRE.

Contents

HCAT Online Safety Policy 2

1. Introduction 2
2. Roles and Responsibilities 2
3. Managing online safety 4
4. Cyber Bullying 4
5. Child on child sexual abuse and harassment 5
6. Grooming and exploitation 6
7. Mental Health 7
8. Online hoaxes and harmful online challenges 7
9. Cyber Crime 8
10. Online safety training for staff 8
11. Online safety and the curriculum 8
12. Use of technology in the classroom 10
13. Use of smart technology 10
14. Educating parents 11
15. Internet access 11
16. Filtering and monitoring online activity 11
17. Network Security 12
18. Emails 12
19. Generative artificial intelligence (AI) 13
20. Social networking 13
21. Breach of this policy 13

Version Number	Version Description	Date of Revision
1	Original	September 2019
2	Reviewed and Rebranded	September 2025
3	Updated in line with KCSIE 2026	July 2026

HCAT Online Safety Policy

1. Introduction

The HCAT Online Safety Policy reflects significant updates to align with the latest regulatory requirements and emerging technological challenges. The policy maintains its foundation of addressing four key risk areas: Content, Contact, Conduct, and Commerce, while introducing several important updates. Key new additions include:

- Enhanced focus on mental health impacts of online activity
- Expanded guidance on smart technology usage in schools
- Strengthened approach to cyber security, including implementation of DfE's cyber security standards
- More detailed guidance on the use of generative AI in education
- Updated responsibilities for Trust Executive Team regarding resource allocation and incident monitoring

Notable updates to existing sections include:

- Refined roles and responsibilities, particularly for Senior Leaders and ICT support
- Enhanced monitoring requirements for online safety incidents
- Strengthened guidance on filtering systems aligned with new DfE standards
- Updated approach to remote learning safety
- Consolidated Acceptable Use Agreement covering all stakeholders

HCAT understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning across our schools. The use of online services is embedded throughout our schools; 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, age-inappropriate apps and games, self-harm and suicide content, 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, and in-app purchases.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Roles and Responsibilities

The Trust Executive Team is responsible for:

- Reviewing this policy regularly to ensure compliance with relevant laws and statutory guidance.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that online safety is a running and interrelated theme throughout the Trust's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

• Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
• Allocating sufficient resources to enable effective implementation
• Monitoring online safety incidents across the Trust to identify trends and areas for improvement

The Principal / Executive Leader / Head of School is responsible for:

• Taking the lead responsibility for online safety in the school
• Supporting the DSL by ensuring they have enough time and resources
• Ensuring staff receive regular, up-to-date online safety training
• Ensuring online safety practices are audited and evaluated
• Supporting staff to ensure online safety is embedded throughout the curriculum
• Organising engagement with parents regarding online safety
• Working with the DSL and ICT support to conduct half-termly reviews of this policy
• Reporting to Trustees and Trust leaders regarding online safety risks, incidents and trends.
• Acting as the named online safety lead in school
• Maintaining detailed records of online safety incidents
• Working with staff, parents and pupils to maintain online safety
• Reviewing and updating online safety procedures
• Monitoring online safety incidents to identify trends
• Leading the response to online safety incidents
• Ensuring that this policy is effective within school
• Ensuring their own knowledge of online safety issues is up to date.
• Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
• Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them
• Regular monitoring of online safety arrangements in their school

ICT support is responsible for:

• Providing technical support for online safety measures
• Implementing appropriate security measures
• Ensuring filtering and monitoring systems are updated
• Supporting staff with technical aspects of online safety
• Maintaining network and device security
• Regular security testing and updates

All staff members are responsible for:

• Maintaining awareness of current online safety issues
• Following all policies and procedures related to online safety
• Modelling good online behaviours
• Reporting concerns via established channels
• Engaging with online safety training

3. Managing online safety

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

The Principal / Executive Leader/Head of School has overall responsibility for the school's approach to online safety, with support from their senior leaders and the DSL, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The Principal / Executive Leader/Head of School / DSL should liaise with the police or children's social care, and the Child Exploitation and Online Protection Centre (CEOP) for support responding to harmful online sexual behaviour. The importance of online safety is integrated across all school operations in the following ways:

• Staff 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 on the topic of remaining safe online
• Parents are regularly engaged through workshops and updates
• Regular reviews of infrastructure and procedures

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 HCAT Safeguarding and Child Protection Policy.

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

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The Principal / Head of School / 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 Principal / Head of School / DSL will balance the victim's wishes against their duty to protect the victim and other young people.

Concerns regarding a staff member's online behaviour are reported to the Principal / Head of School, who decides on the best course of action in line with the relevant policies. If the concern is about the Principal / Head of School, it is reported to the CEO.

Where there is a concern that illegal activity has taken place, the Principal / Head of School / DSL contacts the police.

All online safety incidents and the school's response are recorded via the online safeguarding system CPOMS

4. Cyber Bullying

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

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips
- The creation, sharing or distribution of AI-generated images, videos or audio designed to humiliate, abuse, impersonate or target another person, including deepfakes.

- Silent or abusive phone calls
- Threatening or bullying emails
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites
- Abuse between young people in intimate relationships online
- Discriminatory bullying online

The school 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 for pupils and the Dignity at Work Policy for staff.

5. 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 and will remain aware that pupils are less likely to report concerning online sexual behaviours. 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
• The creation, sharing or distribution of AI-generated intimate images or videos (deepfakes or "deep nudes").
• 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 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 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.

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.

6. Grooming and exploitation

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

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

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

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. Senior Leaders will ensure that KCSIE training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

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

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

While child sexual exploitation (CSE) may involve physical sexual abuse or violence, it can also occur through online means. Online platforms may be used to groom, coerce, or manipulate children into engaging in sexually exploitive behaviour, including the creation or sharing of indecent images, involvement in sexualised conversations or being drawn into prostitution or trafficking.

Child criminal exploitation CCE 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 Principal / Head of School / DSL without delay.

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 understand the factors that can make certain pupils more vulnerable to radicalisation and are expected to remain vigilant for any signs that a pupil may have been exposed to, or is being influenced by, radicalising materials or individuals.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the Principal / Head of School / DSL, without delay. They will consider the most appropriate course of action, including whether a Prevent referral is required.

7. 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 Principal / Head of School / 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.

8. Online hoaxes and harmful online challenges

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

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

The Principal / Head of School / 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 Principal / Head of School / DSL 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 Principal / Head of School / DSL assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate. The Principal / Head of School / DSL 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.

9. Cyber Crime

Cyber-crime is criminal activity committed using computers and/or the internet.

There are two key categories of cyber-crime:

• Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

• Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to 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 Trust will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

The Trust will implement it's cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

In addition, the school will implement a cyber awareness into the curriculum for pupils and training for staff to ensure that they understand the basics of cyber security and protecting themselves from cyber crime.

10. Online safety training for staff

The Trust will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. 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. Staff will be trained in how to record and report incidents via the online safeguarding system CPOMS.

11. Online safety and the curriculum

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

• Computing
• PSHE
• RSHE

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

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

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- Understanding AI-generated content, deepfakes, misinformation, impersonation and manipulation.
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.
The Trust is 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.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the DSLs. SENCO, designated teacher for LAC, computing leads work together to ensure the curriculum is tailored so these pupils 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

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

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson

or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

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

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the 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.

12. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- Email
- Cameras
- AI

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, supported by ICT support always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law. Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

While the school recognises 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.

Staff will use all smart technology and personal technology in line with the school's Staff code of conduct.

Pupils will not be permitted to use smart devices or any other personal technology whilst in school.

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.

The school will seek to ensure that it is 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.

14. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Through face to face training sessions, parents are provided with information about the school's approach to online safety and their role in protecting their children.

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.
- AI-generated content, deepfakes and emerging online risks.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

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

- Parents' evenings
- Twilight training sessions
- Online resources

15. Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and marked as being read the Acceptable Use Agreement. The network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

The Trust Executive Leadership will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. They will also ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Trust 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. Relevant leaders, DSLs and staff will understand the filtering and monitoring systems in place, their role in responding to alerts and how concerns should be escalated.

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. ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

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

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the

Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the 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 school's network and school-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.

Filtering and monitoring arrangements will be formally reviewed and documented at least annually, and sooner where emerging risks, incidents or technological developments require.

17. Network Security

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

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

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Two factor authentication is used to protect and support usage.

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

18. Emails

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

Staff members and pupils are required to block spam and junk mail, and report the matter to ICT support. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened. The Trust organises annual training 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 are managed in line with the Cyber-security Response Plan.

19. Generative artificial intelligence (AI)

The Trust will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to 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 recognises that generative AI may present safeguarding risks including misinformation, manipulation, deepfakes, harmful content, impersonation, grooming, exploitation and online abuse. Any concerns relating to AI-generated content involving pupils will be managed in accordance with the Safeguarding and Child Protection Policy and Child-on-Child Abuse Policy.

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

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

The school will make use of Artificial Intelligence Usage Policy and 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.

20. Social networking

Personal use

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

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

Pupils are taught about the age limits to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

21. Breach of this policy

Any breach of this policy by employees of the Trust will be taken seriously and could result in formal action being taken in accordance with the Trusts Disciplinary Policy, up to and including dismissal.