



E-SAFETY POLICY

May 2023-24

Potter Street Academy

Part of the Passmores Co-operative Learning Community

Contents:

Statement of Intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Peer on Peer sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Online safety training for teaching staff
11. Online safety and the curriculum
12. Use of technology in the classroom
13. Use of smart technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Generative artificial intelligence (AI)
20. Social networking
21. The school website
22. Use of devices
23. Remote learning
24. Monitoring and review
25. Appendix 1: Personal and Sensitive Data Security – Do's and Don'ts for all staff
26. Appendix 2: Child-Centred Policing Flowchart

The policy is based on the model by The SchoolBus, released in April 2023

The PCLC Local Governing body reviewed the policy in May 2023

The Trustees reviewed and approved the policy on 24th May 2023. The policy will be reviewed annually, or sooner if updates to legislation are made.

Statement of intent

Potter Street Academy 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 school; 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. Our school 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.

Potter Street Academy has assigned staff to the following roles:

Designated Safeguarding Lead (DSL) -	Emma Bloomfield
E-safety Officer -	Luke Hammond
Data Protection Officer (DPO) -	Tina Sparrow
IT Manager -	Ashley Alderson
	Luke Hammond

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- 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'

2. Roles and responsibilities

The Trust Board is responsible for:

Ensuring that this policy is effective and complies with relevant laws and statutory guidance.

Ensuring the DSL's 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.

Ensuring that there are appropriate filtering and monitoring systems in place.

Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- 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, e-Safety Officer 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.

Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.

Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

Working with the e-Safety Officer and Trust Board to update this policy on an annual basis.

The e-safety officer is responsible for:

Taking the lead responsibility for online safety in the school.

Acting as the named point of contact within the school on all online safeguarding issues.

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 SENCO and ICT 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.

Ensuring appropriate referrals are made to external agencies, as required.

Keeping up-to-date with current research, legislation and online trends.

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 pupils and staff.

Ensuring all members of the school community understand the reporting 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.

Working with the headteacher, DSL and Trust Board to update this policy on an annual basis.

IT technicians are responsible for:

Providing technical support in the development and implementation of the school's online safety policies and procedures.

Implementing appropriate security measures as directed by the IT Manager.

Ensuring that the school's filtering and monitoring systems are updated as appropriate.

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.

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 e-safety officer has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

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

- Staff receive regular training
- Staff receive regular 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

Handling online safety concerns

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

Staff will be aware 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.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Dealing with Safeguarding Allegations Against Adults Policy, and Disciplinary Policy

and Procedures. If the concern is about a headteacher, it is reported to the chair of the local governing body.

Concerns regarding a pupil's online behaviour are reported to the e-safety officer, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour for Learning Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contact 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 e-safety officer will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy and using the Child-Centred Policing Cyber Crime flowchart.

All online safety incidents and the school's response are recorded by the e-safety officer.

4. Cyberbullying

Cyberbullying can include 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 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.

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 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 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 responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the e-safety officer, who will investigate the matter in line with the Harmful Sexual Behaviour & Peer-on-peer Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

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

Staff will be aware that grooming often takes place online and that 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 e-safety officer without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

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

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty 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 e-safety officer without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy.

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 e-safety officer 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 Student Mental Health Policy.

8. Online hoaxes and harmful online challenges

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

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

in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the 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 e-safety officer immediately.

The e-safety officer 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 e-safety officer 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 e-safety officer and the headteacher will decide whether each proposed response is:

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

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

The e-safety-officer and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

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 e-safety officer 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 e-safety officer and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The e-safety officer 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.

The e-safety officer acts as the first point of contact for staff requiring advice about online safety.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum.

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

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

How to evaluate what they see online

How to recognise techniques used for persuasion

What healthy and respectful relationships, including friendships, look like

Body confidence and self-esteem

Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts

Acceptable and unacceptable online behaviour

How to identify online risks

How and when to seek support

Knowledge and behaviours that are covered in the government's online media literacy strategy

How to identify when something is deliberately deceitful or harmful

How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

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

The e-safety officer 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.

Relevant members of staff, e.g. the SENCO 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

Where does this organisation get their information from?

What is their evidence base?

Have they been externally quality assured?

What is their background?

Are they age appropriate for pupils?

Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher decides 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 e-safety officer 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 e-safety officer 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 asking questions, and are not worried about getting into trouble or being judged.

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

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

12. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets

- 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 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.

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

Staff will use all smart technology and personal technology in line with the school's ICT Acceptable Use Policy (see Appendix 1, Staff Code of Conduct).

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school'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.

Where it is deemed necessary, the school will ban 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 for Learning 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 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 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents are 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.

The school website has a dedicated area for online safety for parents.

The newsletter is often used to alert parents to current issues.

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. youth produced sexual imagery.
- Cyberbullying
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

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

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

Parents' evenings

training sessions

Newsletters

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 signed the Acceptable Use Agreement.

All members of the school community are encouraged to use the school'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.

16. Filtering and monitoring online activity

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

The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

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

Deliberate breaches of the filtering system are reported to the e-safety officer 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 for Learning 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 are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the e-safety officer who manages the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

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

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

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in class, year or key stage and above are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to

be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

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

Full details of the school's network security measures can be found in the Cyber-security Policy.

18. Emails

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

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 and sign 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 alert IT technicians if they feel a particular email contains a threat to recipients. 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. ICT technicians organise an annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly 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 Action Plan.

19. Generative artificial intelligence (AI)

The school 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 school 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 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 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.

Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.

Pupils are regularly educated on the implications of posting personal data online outside of the school.

Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole. This includes not posting images of students on any platform where permission to do so has not been expressly granted.

Staff are not permitted to publish comments about the school which may adversely affect its reputation.

Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

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

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

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

Use on behalf of the school

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

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

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.

21. The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website in accordance with requirements of the UK GDPR.

Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully and will not be posted until authorisation from parents has been received.

22. Use of devices

School-owned devices

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

Laptop

Tablet

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

School-owned devices are used in accordance with the Acceptable Use Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices.

ICT technicians and the e-safety officer will review and authorise any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission from an ICT technician or the e-safety officer.

Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour for Learning Policy respectively.

Personal devices

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

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

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

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Dealing with Safeguarding Allegations Against Adults Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Dealing with Safeguarding Allegations Against Adults Policy.

Pupils are not permitted to use their personal devices during lesson time or when moving between lessons. If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

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

Pupils' devices can be searched, screened and confiscated in accordance with the Behaviour for Learning Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the e-safety officer or DSL.

23. Remote learning

All remote learning is delivered in line with the school's Remote Education Policy.

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable ‘public’ living area within the home with an appropriate background – ‘private’ living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the headteacher, in collaboration with the SENCO.

Pupils not using devices or software as intended will be disciplined in line with the Behaviour for Learning Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

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

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

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

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

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

23. Monitoring and review

This policy will be reviewed on an annual basis by the e-safety officer.

The policy was ratified by the Trust Board on 24th May 2023 following consultation with the Local Governing Body.

Appendix 1: Personal and Sensitive Data Security – Do's and Don'ts for all staff

Passwords – Do

- use a strong password (see Information Systems and Social Media policy for information).

Passwords – Don't

- share your passwords with anyone else or write them down
- save passwords in web browsers if offered to do so.

Devices – Do

- try to prevent people seeing you enter passwords or view sensitive information
- log-off / lock your device when leaving it unattended.

Devices – Don't

- use personal devices to view trust-related or pupil data.

Sending and sharing - Do

- be aware of who you are allowed to share information with. Check with the DPO if you are not sure, who will check that third parties are GDPR-compliant.
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any personal or sensitive data outside of the trust, which should be **avoided at any cost** and only done with explicit permission from the DPO or IT Manager.

Sending and sharing – Don't

- use removable media (USB drives, CDs, portable drives) for any purpose in school.
- send personal or sensitive information by email unless it is encrypted and use the systems that you are told to use.

Accessing / saving data – Do

- only attempt to access data you are allowed to and save it on locations where the trust knows that data is stored (the trust must know where all data is and be able to access it at all times).

Working on-site – Don't

- leave personal or sensitive information unattended; lock it away in lockable drawers or logoff or lock your work station.
- let strangers or unauthorised people into staff areas or on your PC or device.
- position screens where they can be read from outside the room.

Working off-site – Do

- only take information offsite when you are authorised to and only when it is necessary.

- make sure you sign out completely from any services you have used.
- ensure you save to the appropriate directory to enable regular backups.
- ensure that it is protected offsite in the ways referred to above, access data remotely instead of taking it off-site using approved secure systems.
- only take paper copies off site if it is absolutely necessary and ensure they are not left in a car or public area and are stored safely at home.

General Information and Guidance

What is personal data: any information relating to an identifiable living person, e.g. name, contact details, ID numbers, attendance and assessment information, financial information

What is sensitive personal data: includes information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and whether a child is looked-after, has SEN, or is eligible for free school meals

- ✓ Remember that data protection laws DO NOT stop you from reporting safeguarding concerns
 - You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this
- ✓ Only collect the information you actually need
 - When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
 - If you don't need it, or only want it "just in case", don't collect it
 - If you've already collected personal information that you don't need, delete it
- ✓ Keep personal data anonymous, if possible
 - For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to
 - This is particularly important with photographs for external use – if you have an image of a child, don't attach their name to it unless you have explicit consent to do so (student services can give this information or it is available on SIMS on Tab 12 – Parental Consent)
- ✓ Think before you put information up on the wall
 - If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments. Still only display the information you really need to

- If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil (if aged 13 or over) or check SIMS to ensure we have consent to display it
- ✓ Photograph consent has been sought in the following areas and is available in Tab 12 – Parental Consent on SIMS.
 - School Website.
 - School Prospectus
 - Internal displays (SIMS, Reward Board etc.)
 - School videos
 - Press Releases
 - School Newsletters
 - School Apps
 - Twitter

Appendix 2: Child-Centred Policing Flowchart

CYBER CRIME

Definition: Cyber Dependent Activity includes: Unauthorised access to computers, Denial of Service or other computer interference and impairment, Acts causing serious damage to or loss of data, 'Hacking'.

