Bishop Hogarth
Catholic Education Trust

Online Safety Policy

St Joseph's Catholic Primary School

Bishop Hogarth Catholic Education Trust

Document Management:	
Date Policy Approved:	8 January 2015
Date Amended:	October 2024
Next Review Date:	October 2027
Version:	4
Approving Body	Standards Committee

Change Log	
Update:	Updated to reflect Cyber Security Standards for Schools & Colleges, Filtering and Monitoring Standards for Schools & colleges and Keeping Children Safe in Education
Location:	**Statement of intent** **Legal Framework** **Roles and responsibilities** **Cyberbullying** **Cyber-crime** **Filtering and monitoring** **Network security** **Use of devices & Smart technology**
Summary Date:	**21/10/2024**
Completed by:	**Julian Kenshole – Dorector of Governance**

Statement of intent

Bishop Hogarth understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students / pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, 'to such extent as is reasonable', to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties within schools for any such inappropriate behaviour. This may be pertinent to incidents of cyber-bullying, or other online safety incidents involving pupils or students covered by this policy, which may take place out of school.

Our schools will:

- Support parents in helping their children engage safely and responsibly with social media
- Encourage all members of the community, including parents, to use social media responsibly
- Develop whole-school policies and practices for combating bullying, including cyberbullying and sexting (also known as youth produced sexual imagery)
- Ensure that sanctions are appropriate and consistent
- Ensure routes for reporting incidents are clear

[Updated] 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'
- **[Updated]** DfE 'Keeping children safe in education'
- **[Updated]** Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- **[Updated]** DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- **[New]** DfE' (2024) 'Cyber security standards for schools and colleges'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Acceptable Use Agreement
- Safeguarding Children / Child Protection Policy
- Information Security Policy
- Remote Learning Policy
- Relationships & Sex Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Use of Photographic and Video Images of Children Policy
- Political Indoctrination & Visiting Speaker Policy
- Promoting Positive Health & Well-being Policy
- E Mail Policy
- **[New]** Cyber Security Response Plan

[Updated] Roles and responsibilities

Directors

Directors are responsible for:

- the approval of the Online Safety Policy and for monitoring its effectiveness.
- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead's (DSL) remit covers online safety.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff receive regular safeguarding and child protection training, including online safety.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant Trust policies have an effective approach to planning for, and responding to online challenges.

A member of the Board of Directors has taken on the role of Safeguarding Director. The role of the Safeguarding Director will include:

- monitoring and review of the annual safeguarding audit
- reporting to the Board of Directors

Local Governing Committee

Governors are responsible for the implementation of the Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Local Governing Committee receiving regular information about online safety incidents through their Headteacher report and through an annual review and risk assessment of the school approach to online safety.

A member of each Local Governing Committee has taken on the role of Safeguarding Governor. The Safeguarding Governor will:

- have regular meetings with the academy's Designated Safeguarding Lead
- review online safety as part of the annual safeguarding audit
- report issues to relevant Governors meeting(s)

Headteacher

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 and the deputy DSL(s) 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 that the school approaches to online safety are reviewed.
- 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.

[Updated] Designated Safeguarding Lead

The Designated Safeguarding Lead 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 IT staff.
- 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.
- **[Updated]** Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- **[New]** Understanding the purpose of record keeping.
- 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.
- Report to the Local Governing Committee about online safety on an annual basis including a review of the school and Trust approach to online safety supported by a risk assessment. A free online safety self-review tool for schools can be found via the 360 safe website at https://360safe.org.uk/

IT Director:

The IT Director is responsible for ensuring that the:

- Trust's IT infrastructure is secure and is not open to misuse or malicious attack
- Network users can only gain access through Trust provided credentials and adhere to the Acceptable Use Policy
- Trust's filtering protocols are applied and updated on a regular basis
- They keep up to date with online safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Use of the Trust's IT network is regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Safeguarding Lead and Headteacher for investigation and action.
- Providing technical support in the development and implementation of online safety procedures and controls.

Staff

All staff members are responsible for:

- Taking responsibility for the security of IT 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.
- Having read and understood the staff Acceptable Use Policy and Code of Conduct.
- Reporting any 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

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.

Parents / Carers

Parents / Carers can play a crucial role in ensuring that their children understand the need to use the internet or mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns /resources including Parent Info http://parentinfo.org/. Parents and carers will be responsible for:

- familiarising themselves with the Student Acceptable Use Agreement
- Supporting their child in the safe use of mobile devices, social networking sites and the web

Managing online safety

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

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

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

- Staff receive regular training including at induction
- Staff receive regular safeguarding updates including online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum and included as a topic during assemblies

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 Safeguarding Children / Child Protection Policy.

Concerns regarding a staff member's online behaviour will be reported to the headteacher or the most senior member of staff if the headteacher is not present, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher it will be reported to the Chief Executive Officer.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and IT staff, and manages

concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding Children / Child Protection Policy.

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

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

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

[Updated] **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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

[New] 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 Behaviour Policy.

[Updated] Child-on-child sexual abuse and harassment

[Updated] All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts

- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school 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 and the Social Media Policy.

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

[Updated] Grooming and exploitation

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

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

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

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

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

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding Children / Child Protection Policy.

Radicalisation

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

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as detailed in their Prevent Duty training. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

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

[Updated] Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Key Staff will receive Mental Health First Aid Training and each school will appoint a Senior Mental Health Lead. A strategic whole school approach to mental health will be adopted in line with the Promoting Positive Health & Well-being Policy.

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 some can potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

[Updated] Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

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

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

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

[Updated] 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 DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

[New] The school/Trust will implement the DfE's 'Cyber security standards for schools and colleges' and implement training for staff and pupils to ensure that they understand the basics of cyber security and protecting themselves from cybercrime. Training will be undertaken at least annually. The NCSC have downloadable copies of cyber security information cards for schools which provides practical tips for those working in education.

[Updated] Online safety training for staff

[Updated] The DSL 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.

Online safety and the curriculum

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

- RSE
- Health education
- PSHE
- Citizenship

- ICT

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

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

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The DSL is involved with the development of the school's online safety curriculum which will be designed through reference to the risks that pupils may face. The School will have reference to Teaching Online Safety in School Guidance published by the Department for Education in the design of the curriculum. The following resources may also be useful in teaching online safety:

- DfE advice for schools: teaching online safety in schools;
- UK Council for Internet Safety (UKCIS) Education for a connected world;
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people;
- The UKCIS external visitors guidance will help schools to ensure the maximum impact of any online safety sessions delivered by external visitors;
- National Crime Agency's CEOP education programme: Thinkuknow;

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 SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The 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. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate in accordance with the Political Indoctrination & Visiting Speaker Policy.

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 Children / 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 Children / Child Protection Policy.

Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- Intranet
- 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.

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

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 receive a copy of the acceptable use policy and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content. Parents will be provided a number of resources including referral to ThinkuKnow which provides on line resources and advice to parents and carers.

Internet access

Pupil and staff are reminded when they log on to their computer of Acceptable Use terms.

[Updated] Filtering and monitoring online activity

[Updated] The Trust ensures the school's IT 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'. The Trust ensures that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

[New] 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 filtering and monitoring systems used will be appropriate to pupil ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Requests to make changes to the filtering system are directed through the IT department. Prior to making any changes to the filtering system IT staff will review the request and site. Any changes made are recorded within the system. Reports of inappropriate websites or materials are made to the IT department immediately, who investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and IT Department, 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.

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 that they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Safeguarding Children / Child Protection Policy.

[Updated] Network security

[Updated] Technical security features, such as anti-virus software, are kept up-to-date and managed by the IT department. Firewalls are switched on at all times. The IT department reviews the firewalls on a continuous basis to ensure they are running correctly, and to carry out any required updates. Multi-factor Authentication is in use.

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

All members of staff have their own unique usernames and private passwords to access the school's systems. Staff members and pupils are responsible for keeping their passwords private.

Users inform IT department if they forget their login details, who will arrange for the user to access the systems under different login details. Users (both staff and pupils) are aware through the Acceptable Use terms that they are not permitted to share their login details with others and are not allowed to log in as another user at any time.

[Updated] Users are required to lock access to devices and systems when they are not in use and adhere to the following good practice:

Do's

- Ensure your device operating system is kept up to date and patched with the latest security updates.
- Ensure your software applications or apps are up to date with the latest versions.
- Ensure your device has anti-virus software / malware protection installed.
- Keep your personal and work files and activities separate and organised.
- Use Muti-Factor Authentication (MFA) and use strong passwords to access your work account.
- If possible, encrypt your device to prevent access if your device is stolen.
- If anything is suspicious, let the IT team know immediately.

Don’ts

- Allow any other person to access work related data.
- Save or keep work related data on personal devices.
- Do not disable anti-virus software.
- Do not connect to untrusted computer networks.
- Do not share passwords, Multi-Factor Authentication requests / codes, or access credentials.

Full details of the school’s network security measures can be found in the Information Security Policy

Emails

Staff and pupils will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a ‘valued customer’, ‘friend’ or ‘colleague’?
- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the school asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.
- Is it from a generic email address, such as Gmail or Hotmail?

The IT Director will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam. The IT Director will ensure that the filtering system is neither too strict nor too lenient, to allow the correct emails to be sent to the relevant folders.

The Trust’s monitoring system can detect inappropriate links, malware and profanity within emails.

Social networking

Personal use

Access to social networking sites is filtered as appropriate. 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 and Acceptable Use terms contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy e.g. Staff Code of Conduct and Pupil Behaviour Policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Media Relations Policy. Staff members must be authorised by the headteacher to access to the school's social media accounts.

[Updated] Use of devices & Smart technology

In accordance with Keeping Children Safe in Education each school is required to consider how the use of mobile devices and technology is managed on their premises. This may involve:

- Pupils not being 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.

[New] 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.

[New] 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 as follows:

> **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
>
> **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
>
> **Conduc**t: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
>
> **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

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 and Physical Interventions Policies. 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 confiscated and handed to the police.

Remote learning

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

Safeguarding remains a top priority and a Designated Safeguarding Lead will be available at all times to address any concerns raised through virtual learning and/or onsite learning. The school will ensure that all tasks and activities that the students undertake during periods of remote learning are safe. Students are expected to follow carefully the instructions of their teacher during lessons.

It is important for ensuring online safety and developing a work life balance that:

- Teachers will only communicate through the school-based learning platform
- Staff will not give parents, or students, their mobile number or personal email address
- Teachers will be available during their timetabled lesson and will not respond to communications outside

Monitoring and review

The Trust recognises that the online world is constantly changing, therefore, this Policy will be reviewed within the context of new technologies, threats, harms and legislation when appropriate. The Trust will carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks our children face.