The Bishop Wheeler Catholic Academy Trust

Policy

Online Safety Policy

Published: May 2025

To be reviewed: 2026/27

The Bishop Wheeler Catholic Academy Trust

Our Mission

Outstanding Catholic education for all pupils. As a family of schools, we will enable our young people to develop spiritually, morally, intellectually and personally, putting their faith into action, through serving Christ in others, in the church and in the world around them.

This policy was approved by the Chief Executive Officer on behalf of the of the Trust Board

Signature:

Mr D Beardsley
Chief Executive Officer
Date:20/05/25

Version:		2.0	
Approved by Chief Executive Officer:		20/05/25	
Review Frequency:		Annually	
Revision Date:		2026/27	
Legislation/Category:		Trust Policy	
Version	**Date**	**Description**	**Revision Author/s**
1.0 Published	December 2022	Trust Policy	JJN/MHY/NFR/CCD/CAN/GNE/AAH (Executive Headteacher for the Trust Primary Schools)/ALI (Catholic Lead for the Trust Primary Schools)
2.0	May 2025	Review	JJN/MHY/NFR/SCE/HTN (Executive Headteacher)

Change review

Version	Date	Changes
2.0	May 2025	**Page 3 -** Review changed to Annually **Page 6** - Legal Framework updated **Page 7** – Roles and Responsibilities updated **Page 12** – Classroom use update **Page 13** – Internet Access updated **Page 14 –** Network security updated **Page 14** – Emails updated **Page 15** – Generative artificial Intelligence (AI) added. **Page 18** – Use of personal devices updated **Page 23** - Child on Child abuse updated **Page 24** – Sexting and the sharing of indecent images of children, information added

Online Safety Policy

Contents

1. Introduction 6
2. Legal Framework 6
3. Roles and Responsibilities 7
4. The curriculum 10
5. Staff training 11
6. Educating parents 12

7. Classroom use 12
8. Internet access 13
9. Filtering and monitoring online activity 13
10. Network security 14
11. Emails 14
12. Generative Artificial Intelligence (AI) 15
13. Social networking 15
14. Online hoaxes and harmful online challenges 16
15. The school and Trust websites 18
16. Use of school-owned devices 18
17. Use of personal devices 18
18. Managing reports of online safety incidents 19
19. Responding to specific online safety concerns 19
20. Online sexual violence and sexual harassment between children (child on child abuse) 22
26. Remote learning 26

Definitions

In this policy, unless the context otherwise requires, the following expressions shall have the following meanings:

BWCAT	The Bishop Wheeler Catholic Academy Trust.
Trust, we and our	Covers all the schools within The Bishop Wheeler Catholic Academy Trust and The Bishop Wheeler Catholic Academy Trust Office.
Trust Board	The Directors of the Trust Board.
Academy Council	Governors elected or appointed to individual Academy Councils.
Governors	Governors appointed to the Academy Council of the individual academy.
CEO	The Chief Executive Officer for the Trust.
Executive Headteacher/Headteacher	Executive Headteacher/Headteacher responsible for individual academies.
Academy/schools	Refers to the Academies within BWCAT.
Pupil	Refers to any pupil on roll at any of the BWCAT schools.
Parents	Refers to any person who holds parental responsibility for the pupil
Child and Children	Refers to children and young people under the age of 18 years.
Staff	Means all employees, temporary, casual, agency and contracted staff working for the Trust, volunteers and consultants.
LA	Refers to the Local Authority
DSL	Refers to Designated Safeguarding Lead
DDSL	Refers to Deputy Designated Safeguarding Lead
DSO	Refers to Designated Safeguarding Officer

1. Introduction

BWCAT understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.
The use of online services is embedded throughout the Trust's 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, and racist or radical and extremist views
- **Contact:** Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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

2. 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 (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education'
- 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'
- National Cyber Security Centre (2020) 'Cyber Security: Small Business Guide'
- UK Council for Internet Safety (2020) 'Education for a Connected World

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

- ICT Acceptable Use Policy

- Freedom of Information Policy
- Child Protection and Safeguarding Policy
- RSHE and Health Education Policy
- School Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy

3. Roles and Responsibilities

The Trust Board are 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 (Delegated authority to the CEO).
- Ensuring knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant BWCAT policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

The Executive Headteacher/Headteacher is responsible for:

- Supporting the DSL and 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 that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.

- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Ensuring all members of the school community understand the reporting procedure.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

The DSL (and DDSL's) are responsible for:

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policies.

- 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.
- Understanding the filtering and monitoring processes in place at the school.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCo and ICT provider.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends
- 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.
- Providing regular reports on online safety in school to the Headteacher and/or Academy Council

The ICT manager is responsible for:

The primary schools within the Trust generally outsource their IT support. This policy should be made available to those that provide IT support. It will be the Headteachers responsibility to ensure IT support understand and abide by this policy.
The secondary schools have in house IT support and an ICT Manager, who will also follow the guidelines of this policy.

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- The ICT Manager/ICT Provider undertakes a risk assessment to determine what filtering and monitoring systems are required. An annual review of the systems is carried out by the Designated Safeguarding Lead and the ICT Manager / ICT Provider
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

All staff members are responsible for:

- Maintaining an understanding of this policy
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents are expected to:

- Support their child to be safe online
- Be aware of the ICT Acceptable Use policy on the school website

Pupils are responsible for:

- Adhering to this policy, the ICT 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.

4. The curriculum

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

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently, regardless of the device, platform or app they are using. Online safety teaching is always appropriate to pupils' ages and developmental stages.

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

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- 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 online risks pupils may face online are always considered when developing the curriculum. The DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm. Relevant members of staff work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

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.

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 sections "Managing reports of online safety incidents" and Responding to specific online safety concerns" of this 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 sections "Managing reports of online safety incidents" and "Responding to specific online safety concerns" of this policy.

5. Staff training

All staff receive safeguarding and child protection training, which includes online safety training. Staff receive online safety training during their induction process. All staff receive refresher training every three years.

In addition to this training, staff also receive regular online safety updates as required and at least annually.

The DSL and DDSL's undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DSL and deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff are informed about how to report online safety concerns, in line with sections "Managing reports of online safety incidents" and Responding to specific online safety concerns" of this policy.

The DSL/DDSL's/DSO's acts as the first point of contact for staff requiring advice about online safety.

6. 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 ICT Acceptable Use Agreement when their child starts school and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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

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

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.
Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- School website
- Newsletters
- Online resources

7. Classroom use

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

- Computers
- Laptops
- Mobile Devices
- Internet
- Email

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.

8. Internet access

Pupils, staff and other members of the school community are only granted access to the school's network once they have read and signed the ICT 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.

9. Filtering and monitoring online activity

The ICT Manager/ICT Provider ensures the ICT network has appropriate filters and monitoring systems in place.

The integrity of the school's ICT systems is monitored and alerts regarding potential issues are automatically generated and sent to the ICT Manager / ICT Provider.

The filtering and monitoring systems 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.

Schools ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The ICT Manager/ICT provider undertake 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/ICT Manager.

Reports of inappropriate websites or materials are made to the Headteacher/ICT Manager and the DSL immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the ICT Manager/ICT Provider, who will escalate the matter to the Headteacher.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the school's Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the 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 (The Child Exploitation and Online Centre) 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 Headteacher and BWCAT's Chief Operating Officer (COO) who manage the situation in line with sections "Managing reports of online safety incidents" and "Responding to specific online safety concerns" of this policy.

10. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the ICT Manger/ICT provider, firewalls are switched on at all times.

Staff and pupils are advised not to download or open unfamiliar email attachments.

Staff members and pupils report all malware and virus attacks to the ICT Manager/ ICT provider.

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

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 are not permitted to share their login details with others and are not allowed to log in as another user at any time. In exceptional circumstances pupils may need to share their login details with a parent or legal guardian if they require support.

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

Users inform the ICT Manager/ICT provider if they forget their login details, who will arrange for the user to access the systems under different login details.

If a user is found to be sharing their login details and there are no exceptional circumstances or otherwise mistreating the password system, the Headteacher is informed and decides the necessary action to take.

11. Emails

Access to and the use of emails is managed in line with the BWCAT's ICT Acceptable Use Policy and BWCAT Data protection Policy.

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 ICT Acceptable Use Agreement.

Any emails sent externally that contains sensitive or personal information should be suitably protected at all times. The IT manager/ICT support can offer guidance on how to send confidential e-mails.

Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Pupils and staff are made aware of what a phishing email and other malicious emails might look like, including:

- 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 cyberattacks initiated through emails are to be reported immediately to the Headteacher and the BWCAT Chief Operating Officer (COO)

12. Generative Artificial Intelligence (AI)

The Trust/school prepares pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils’ age.

The Trust/school ensures its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI. The Trust/school takes steps to prevent pupils from accessing or creating harmful or inappropriate content, including through generative AI.

The Trust/school takes steps to prevent personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The Trust/school makes 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.

13. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school and the Trust.

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 close family friends with a parent at the school, staff will follow the safer working practice guidance and the staff code of conduct. Staff 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 ICT Manager/DSL who will make the Headteacher aware and managed in accordance with the relevant policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with BWCAT's ICT Acceptable Use Policy.

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

Staff members should be authorised by the Headteacher to access to the school's social media accounts.

BWCAT's ICT Acceptable Use Policy contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

14. 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 Headteacher ensures that pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content.

The DSL will work with the SENCo to assess whether some pupils, e.g. pupils who have been identified as being vulnerable or pupils with SEND, need additional help with identifying harmful online challenges and hoaxes, and tailor support accordingly.

The school will ensure all pupils are aware of who to report concerns to surrounding potentially harmful online challenges or hoaxes.

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.

The DSL will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.

The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

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.

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:

- Factual and avoids 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 that 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.
- Age-appropriate and appropriate for the relevant pupils' developmental stage.
- Supportive.

15. The school and Trust websites

The Headteacher is responsible for the overall content of their school's website. With support from the BWCAT Head of Governance, they will ensure the content is appropriate, accurate, and up-to-date and meets government requirements.

The BWCAT Chief Operating Officer (COO) is responsible for the overall content of the BWCAT website. Delegating the maintenance and up keep of the website to the appropriate member/s of staff, the BWCAT Head of Governance will ensure all content is relevant, up-to-date and meets all statutory requirements.

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

Personal information relating to staff and pupils is not published on school websites. Images and videos are only posted on the website if consent is gained from the relevant members of staff, pupils and parents.

16. Use of school-owned devices

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. laptops to use during lessons. School-owned devices are used in accordance with the ICT Acceptable Use Policy. All school-owned devices are password protected.

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.

No software, apps or other programmes can be downloaded onto a device without authorisation from the ICT Manager/ICT provider.

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 school Behaviour Policy respectively.

17. Use of personal devices

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

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 procedures for dealing with allegations made against staff.

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 and the pupil's parents will be informed Any concerns about visitors' use of personal devices on the school premises are reported to the Headteacher. If personal devices are used in school, information will be shared with the pupil and parents and an agreement made to ensure responsible use.

18. Managing reports of online safety incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

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.

Concerns regarding a pupil's online behaviour are reported to the DSL/DDSL's/DSO who will investigate concerns with relevant staff members.

Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. school Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher (or delegated staff member) will 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 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.

19. Responding to specific online safety concerns

Cyberbullying

Definition:

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Cyberbullying is the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else.

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

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups/year group class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that

material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, the Headteacher or delegated member of the senior leadership team will decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

Staff must not erase or delete images or files from devices, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable.

If the material is not suspected to be evidence in relation to an offence, staff members must consult with the DSL/Headteacher if they reasonably suspect that its continued existence is likely to cause harm to any person. The Headteacher/DSL in liaison with parents will request that the material is erased.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

20. Online sexual violence and sexual harassment between children (child on child abuse)

The school recognises that child on child abuse can take place online. Examples include the following:

- Consensual or Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation
- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent.

The school will respond to all concerns regarding online child on child abuse, whether or not the incident took place on the school premises or using school-owned equipment.

Concerns regarding online child on child abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Information about the school's full response to incidents of online child on child abuse can be found in the Child Protection and Safeguarding Policy.

21. Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

- A "specified purpose" is namely:
    - Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
    - To humiliate, distress or alarm the victim.

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the BWCAT and its schools. Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

22. Sexting and the sharing of indecent imagery of pupils

Sharing indecent imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 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.

Staff responsibilities when responding to an incident:

- If any adult in school is made aware of an incident involving the consensual or non-consensual sharing of nude or semi-nude images/videos (also known as 'sexting' or 'youth produced sexual imagery'), they must report it to the DSL immediately.

Staff must not:

- View, copy, print, share, store or save the imagery, or ask a pupil to share or download it (if you have already viewed the imagery by accident, you must report this to the DSL)
- Staff must not delete the imagery or ask the pupil to delete it
- Staff must not ask the pupil(s) who are involved in the incident to disclose information regarding the imagery (this is the DSL's responsibility)
- Do not share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any young people involved

DSL Responsibilities:

- Following a report of an incident, the DSL will hold an initial review meeting with appropriate school staff – this may include the staff member who reported the incident and the safeguarding or leadership team that deals with safeguarding concerns.
- This meeting will consider the initial evidence and aim to determine: Whether there is an immediate risk to pupil(s) If a referral needs to be made to the police and/or children's social care
- If it is necessary to view the image(s) in order to safeguard the young person (in most cases, images or videos should not be viewed)
- What further information is required to decide on the best response
- Whether the image(s) has been shared widely and via what services and/or platforms (this may be unknown)
- Whether immediate action should be taken to delete or remove images or videos from devices or online services
- Any relevant facts about the pupils involved which would influence risk assessment If there is a need to contact another school, college, setting or individual Whether to contact parents or carers of the pupils involved (in most cases parents/carers should be involved)

The DSL will make an immediate referral to police and/or children's social care if:

- The incident involves an adult
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example, owing to special educational needs)
- What the DSL knows about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- The imagery involves sexual acts and any pupil in the images or videos is under 13

- The DSL has reason to believe a pupil is at immediate risk of harm owing to the sharing of nudes and semi-nudes (for example, the young person is presenting as suicidal or self-harming)
- If none of the above apply then the DSL, in consultation with the Headteacher and other members of staff as appropriate, may decide to respond to the incident without involving the police or children's social care. The decision will be made and recorded in line with the procedures set out in schools Safeguarding and Child Protection policy.

The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

Imagery will not be purposefully viewed where it will cause significant harm or distress to any pupil involved, in line with the DSL's professional judgement.

Any accidental or intentional viewing of imagery that is undertaken as part of an investigation is recorded.

Where a staff member has accidentally viewed a nude or semi-nude image, the DSL will ensure they are provided with the appropriate support, as viewing nude or semi-nude imagery of pupils can be distressing.

23. Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school will respond to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

24. Online hate

The BWCAT does not tolerate online hate content directed towards or posted by members of the school community.

Incidents of online hate are dealt with in line with the relevant school/Trust policy depending on the nature of the incident and those involved.

25. Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty Training.

26. Remote learning

The school will communicate to parents 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.

The 16 schools in our Trust:

St. Mary's Menston, a Catholic Voluntary Academy

St. Joseph's Catholic Primary School Otley, a Voluntary Academy

Ss Peter and Paul Catholic Primary School, a Voluntary Academy

Sacred Heart Catholic Primary School Ilkley, a Voluntary Academy

St Mary's Horsforth Catholic Voluntary Academy

St. Joseph's Catholic Primary School Pudsey, a Voluntary Academy

St Joseph's Catholic Primary School Harrogate, a Voluntary Academy

St Mary's Catholic Primary School Knaresborough, a Voluntary Academy

St. Stephen's Catholic Primary School and Nursery, a Voluntary Academy

Holy Name Catholic Voluntary Academy

St Roberts Catholic Primary School, a Voluntary Academy

St John Fisher Catholic High School Harrogate, a Voluntary Academy

St Joseph's Catholic Primary School Tadcaster, a Voluntary Academy

Barkston Ash Catholic Primary School, a Voluntary Academy

St Joseph's Catholic Primary School Barnoldswick, a Voluntary Academy

St Wilfrid's Catholic Primary School, a Voluntary Academy

The Bishop Wheeler Catholic Academy Trust

The Bishop Wheeler Catholic Academy Trust is a charity and a company limited by Guarantee, registered in England and Wales.

Company Number: 8399801

Registered Office: Bradford Road Menston, LS29 6AE

Website: www.bishopwheelercatholicacademytrust.org

Tel: 01943 883000

Email: j.johnson@bwcat.org

Chair of the Trust Board: Mrs Helen Mills