"Every child is a unique child of God."

WHINMOOR ST. PAUL'S C of E Primary School

Whinmoor St Paul's (VA) C of E Primary School

Online Safety Policy

Every Child is a Unique Child of God

At Whinmoor St. Paul's Church of England Voluntary Aided Primary School, everything we do is underpinned at all times by the Christian ethos of valuing the individual. We believe that every child is respected as a unique child of God, the future adults in society. We believe children are gifts from God and we are privileged to work with their families and carers, to enable them to live life to the full.

Agreed Date: January 2026

Review Date: January 2027

Signed: Chair of Governors: Mrs R Davies

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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 scam
- **Misinformation –** Misinformation refers to false or inaccurate information that is spread, regardless of intent.
- **Disinformation -** Disinformation refers to false or misleading information deliberately created and spread with the intent to deceive or manipulate people. Unlike misinformation, which can be spread by mistake or without harmful intent, disinformation is a deliberate act of deception.
- **Fake news –** Fake news refers to fabricated or misleading stories presented as if they were legitimate news reports. These stories are often designed to deceive, misinform, or manipulate the audience, and they typically mimic the appearance and structure of legitimate news content. Fake news can be entirely made up, distorted, or taken out of context to serve a particular agenda.
- **Conspiracy theories -** Conspiracy theories are beliefs or explanations that suggest that events or situations are the result of a secret, often sinister, plot by a group of people or organizations. These theories typically claim that those in power are secretly controlling or manipulating events to serve their own hidden agenda, often at the expense of the public. Conspiracy theories are usually not supported by reliable evidence and tend to rely on speculation, distrust, and the rejection of official explanations.

At Whinmoor St Paul's we are also compliant with the cyber security standards for schools when it comes to using generative artificial intelligence safely.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The head teacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head teacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- 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
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- 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'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the head teacher of any concerns or queries regarding this policy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use upon signing in to school.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant. Children will be given a top tips guide on how to stay safe on the Internet. This will take the form of 22 ways to stay safe online – each rule will be taken

at the start of each Computing lesson and will be discussed within the classroom. This will be sent to parents, read and explained to children and will be available on the school website. (See Appendix 1.) Sessions relating to online safety are interweaved into all sessions through the Purple Mash curriculum. 2BeSafe is also used as an activity to teach children about keeping safe online by breaking this down into eight strands. They are;

- Online Bullying
- Online Relationships
- Online Reputation
- Self-image and identity
- Managing information online
- Health, well-being and lifestyle
- Copyright and ownership
- Privacy and security

5. Filtering and Monitoring

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. Within school, the Computing Lead alongside a designated member of SLT (Lea Vaughan) and a designated governor are responsible for ensuring that these standards are met.

Staff within school are responsible for ensuring that they follow the Computing Policy and Online Safety policy. Teaching staff must ensure that the content they access within school both for themselves and with children in school is appropriate. It is the SLT's responsibility to ensure that all staff understand their role, are appropriately trained, follow policies and act on any reports and concerns.

The senior leadership team are responsible for;

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

It is the responsibility of the Computing Lead to check the effectiveness of the filtering systems within school to ensure that the filtering system is working effectively and efficiently. Reports of any concerns based on filtering and monitoring reports are sent to the Computing Lead, shared with appropriate staff and are actioned in line with the safeguarding policy. Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually. Meetings are also held between the DSL's within school and the named Safeguarding governor to discuss the suitability of school's filtering and monitoring system under the DfE's named 'Plan technology for your school service.' This is done at least annually. This is a self-assessment tool which allows us to ensure that our security standards are fit for purpose. Our filtering and monitoring requirements also apply to the use of generative AI in education.

Reporting Concerns over filtering and monitoring of inappropriate content

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

If a website is blocked and a staff member believes it should not be blocked or requires it to be unblocked so that they are able to carry out a lesson, an unblock request form must be submitted to the Computing Lead where it will be considered on a case-by-case basis.

Monitoring allows us to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action and record the outcome. A variety of monitoring strategies are used to minimise safeguarding risks on internet connected devices and include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party which monitors keystrokes typed into devices that are accessing the school network
- physical checks by the Computing Lead using testfiltering.com to check that all filtering is in place and works
- physical checks of searching 'banned' words logged in as both staff and children to check for alerts

Appendix 2 shows the form that will be used whenever a staff member is completing tests on searching for inappropriate words. This will be done when logged in as a staff member and as a child. Whenever the Computing Lead completes these checks, a second staff member will always be present.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Google Classroom.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the head teacher.

7 . Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 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 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.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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. If a child makes a disclosure support will be given, they will be reassured they have done the right thing and advice should be given on how to deal with it appropriately.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. If a pupil agrees to the search, staff can conduct this. If they do not, permission and advice must be sought from the headteacher before examining and removing devices.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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 school's COVID-19 risk assessment

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

8. Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include:

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded

• 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, staff should refer this to the Designated Safeguarding Lead. They should consider referring this into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety. Additional advice can be found at: Cyber Choices, https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices

9. Child on Child Abuse

9.1 – Definition of child-on-child abuse

Peer abuse is behaviour by an individual or group, intending to physically, sexually or emotionally hurt others.

All staff should recognise that children are capable of abusing their peers. All staff should be aware of safeguarding issues from peer abuse including:

- bullying (including cyber bullying – See Section 6)
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm
- sexual violence and sexual harassment
- sexting (also known as youth produced sexual imagery. See Section 9)
- initiation/hazing type violence and rituals.

This abuse can:

- Be motivated by perceived differences e.g. on grounds of race, religion, gender, sexual orientation, disability or other differences
- Result in significant, long lasting and traumatic isolation

9.2 Online Bullying

Online Bullying is the use of technology (social networking, messaging, text messages, email, chat rooms etc.) to harass threaten or intimidate someone for the same reasons as stated above. Online bullying can take many forms

- Abusive or threatening texts, emails or messages
- Posting abusive comments on social media sites
- Sharing humiliating videos or photos of someone else
- Stealing someone's online identity
- Spreading rumours online
- Trolling – sending someone menacing or upsetting messages through social networks, chatrooms or games
- Developing hate sites about another person
- Prank calls or messages
- Group bullying or exclusion online
- Anonymous messaging
- Encouraging a young person to self-harm
- Pressuring children to send sexual messages or engaging in sexual conversations

See Section 6 for advice on how to handle a cyberbullying incident.

9.3 – Sexting

The term 'sexting' relates to the sending of indecent images, videos and/or written messages with sexually explicit content; these are created and sent electronically. They are often 'shared' via social networking sites and instant messaging services.

Upskirting: typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Anyone of any gender, can be a victim.

See Section 9 for advice on how to handle a sexting incident.

Staff should consider the seriousness of the case and, if necessary, inform the Designated Safeguarding Lead before taking any further in-school actions for incidents of peer-on-peer abuse. Incidents should always be recorded on CPOMS.

10. Sharing of nude/ semi-nude photos

10.1 – What does 'sharing nudes and semi-nudes' mean?

This advice uses the term 'sharing nudes and semi-nudes' to mean the sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline.

The term 'nudes' is used as it is most commonly recognised by young people and more appropriately covers all types of image sharing incidents. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated. Such images may be created and shared consensually by young people who are in relationships, as well as between those who are not in a relationship. It is also possible for a young person in a consensual relationship to be coerced into sharing an image with their partner. Incidents may also occur where:

- children and young people find nudes and semi-nudes online and share them claiming to be from a peer
- children and young people digitally manipulate an image of a young person into an existing nude online
- images created or shared are used to abuse peers e.g. by selling images online or obtaining images to share more widely without consent to publicly shame

The sharing of nudes and semi-nudes can happen publicly online, in 1:1 messaging or via group chats and closed social media accounts. Nude or semi-nude images, videos or live streams may include more than one child or young person. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents involving children and young people complex.

10.2 – Handling incidents – initial response

When an incident involving nudes and semi-nudes comes to staff must follow the guidance below:

- the incident should be referred to the DSL as soon as possible

- the DSL should hold an initial review meeting with appropriate staff. This may include the staff member(s) who heard the disclosure and the safeguarding or leadership team who deal with safeguarding concerns
- there should be subsequent interviews with the children or young people involved (if appropriate)
- parents and carers should be informed at an early stage and involved in the process in order to best support the child or young person unless there is good reason to believe that involving them would put the child or young person at risk of harm
- a referral should be made to children's social care and/or the police immediately if there is a concern that a child or young person has been harmed or is at risk of immediate harm at any point in the process

The circumstances of incidents can vary widely. If at the initial review stage a decision has been made not to refer to police and/or children's social care, the DSL should conduct a further review (including an interview with any child or young person involved) to establish the facts and assess the risks, referring back to any relevant assessment tools.

10.3 Supporting the young person involved

Children and young people who have had their nudes or semi-nudes shared publicly should be:

- reassured that they have done the right thing by speaking to an adult and that the education setting and other adults are there to help
- advised:
    - to use the IWF and Childline's Report Remove tool. Report Remove helps children and young people to report an image shared online, to see if it is possible to get the image removed.
- on how to report sexual images or videos on individual sites to get them taken down. If the image has been shared via a mobile, they should be informed that they can contact the mobile phone operator to have a mobile number changed as this may stop others from contacting them
- to speak to the school if they are concerned about any bullying behaviour

Children and young people who have been sent a nude or semi-nude should be:

- reassured that they have done the right thing by speaking out and that the education setting and other adults are there to help
- asked whether it was sent by an adult or another child or young person and if they requested the photo or if it was sent unsolicited
- advised:
    - on the importance of reporting it online if it has been shared
    - on the importance of not sharing the image further
    - if they asked to receive the photos, explain that they should not put pressure onto others to do things that they are uncomfortable with

Children and young people who have shared another child's or young person's nudes or semi-nudes should be:

- asked:
    - whether they asked for the photo or were initially sent it without requesting
    - who the image has been sent to and where it has been shared. DSL to agree next steps for taking the image down, including deleting the image from their phone or any social media accounts and reporting it to service providers
    - about their motivations for sharing the photo and discuss what they could have done differently. If they have reacted to an upsetting incident, such as the break-up of a relationship, by sending the photo onwards, talk about how they could have managed their feelings in a healthier and more positive way. Emphasise that whatever the reason, it is always wrong to share nudes and semi-nudes of another child or young person. This can be used as an opportunity to discuss the importance of consent and not putting pressure on others to take or share nudes and semi-nudes
- advised on the law on the sharing of nudes and semi-nudes

Staff should not ask to view, copy, print, share, store or save the imagery. If staff view the imagery by accident this should be reported to the DSL.

11. Sexting

11.1 – Definition of 'sexting'

There are a number of definitions of sexting but for the purpose of this advice sexting is simply defined as images or videos generated:

• by children under the age of 18, or

• of children under the age of 18 that are of a sexual nature or are indecent.

These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know. There are many different types of sexting and it is likely that no two cases will be the same.

11.2 – Handling an incident – initial response

Sexting disclosures should follow school's normal safeguarding practices. A child is likely to be very distressed, especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need support during the disclosure and after the event.

If the content is on a mobile device, it can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography, inline with the Education act of 2011 (See Section 6.3.) Devices can be searched if the children gives permission and if they do not, staff must consult with the headteacher to be granted permission.

Staff should never view the image unless there is a clear reason to do so, send, share, copy or save the image anywhere. Children should not be allowed to do any of the above either. Materials should not be moved from one place to another.

11.3 – Dealing with the incident

Whoever the initial disclosure is made to must act in accordance with the school's Safeguarding Policy, ensuring that the Designated Safeguarding Leads are involved in dealing with the incident. The DSL should always record the incident using the school's Safeguarding Concerns Form and also log the incident on CPOMS. There may be instances where the image needs to be viewed and this should be done in accordance with protocols. The best interests of the child should always come first; if viewing the image is likely to cause additional stress, professionals should make a judgement about whether or not it is appropriate to do so.

There may be a multitude of reasons why a child has engaged in sexting – it may be a romantic/sexual exploration scenario or it may be due to coercion. It won't always be appropriate to inform the police; this will depend on the nature of the incident.

12. Acceptable use of the internet in school

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. Any suspicious searches will be flagged and a report will instantly be sent to the headteacher and the Computing Lead. An overall usage report is sent weekly to the headteacher and the Computing Lead. The school expects staff to lead by example and therefore should not make or receive personal calls, or texts (via mobile phone or smart watch), whilst children are present or during contact time.

13. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices into school, but are not permitted to use them during the school day. Pupils who walk home on their own in Year 5 are also permitted to bring phones into school but they, again, must not be used throughout the school day. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

14. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

If staff have any concerns over the security of their device, they must seek advice from the IT lead.

15. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. Training

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse

- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

17. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Computing Policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Remote learning policy

Appendix 1 : Online Safety -Twenty Two Top Tips for Staying Safe Online

Twenty-two ways to stay safe online

1. ***I learn online*** – I use the internet to help me learn online and schoolwork and have fun.
2. ***I ask permission*** –At home and school, I only use the tablet, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. If I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. I never give personal information to anybody I meet online.
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. If I am not sure, I always ask an adult.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I must not share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life and that a trusted adult knows about. I never speak to people who I do not know or do not have permission to speak to.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are and I must ask a parent or carer or trusted adult.
11. ***I only meet an online friend if I am allowed to*** - I must get permission from my parent or carer and I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say 'no' online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I don't give out private information to anyone. I don't turn on location unless my parent or carer gives me permission.

17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever, even if I delete it.
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

Appendix 2: Record of reviewing devices/ internet sites (completing tests on student and staff filtering)

Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....
Date: .....
Reason for investigation: .....
.....
.....
.....

Details of first reviewing person
Name: .....
Position: .....
Signature: .....

Details of second reviewing person
Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)
.....
.....

Web site(s) address/device	*Term searched or reason for concern*

Conclusion and Action proposed or taken
