West View Primary School

Online Safety Policy

Approved by Local Academy Committee: October 2023
Date for Review: October 2024

West View Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood, or causes, of 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. West View Primary School has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal Framework

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

- Voyeurism (Offences) Act 2019 (legislation.gov.uk)
- Guide to the UK General Data Protection Regulation (UK GDPR) | ICO
- Data Protection Act 2018 (legislation.gov.uk)
- Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk)
- Harmful online challenges and online hoaxes - GOV.UK (www.gov.uk)
- Keeping children safe in education - GOV.UK (www.gov.uk)
- Teaching online safety in schools - GOV.UK (www.gov.uk)
- Searching, screening and confiscation at school - GOV.UK (www.gov.uk)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
- Education for a Connected World - GOV.UK (www.gov.uk)
- Cyber Security: Small Business Guide (PDF Version) - NCSC.GOV.UK

Local information regarding Online Child Abuse can be found here: Online Child Abuse - Tees Safeguarding Children Partnerships' Procedures (teescpp.org.uk)

This policy operates in conjunction with the following school policies:

- Acceptable Use
- Allegations of Abuse Against Staff
- Anti-Bullying
- Behaviour
- Child-On-Child Abuse
- Computing

- Data Protection
- Disciplinary
- PREVENT
- PSHE
- Relationships, Sex and Health Education (RSE)
- Safeguarding
- Social, Emotional and Mental Health (SEMH)
- Staff Behaviour/Code of Conduct
- Whistleblowing

Roles and Responsibilities

The Local Academy Committee will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring that the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with the Headteacher, ICT staff and service providers.
- 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.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Headteacher/DSL will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies, procedures, the curriculum, training and safeguarding practices.
- Supporting the deputy DSLs 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 ongoing safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents, carers and the wider community to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with ICT technicians to conduct regular light-touch reviews of this policy.
- Working with the Local Academy Committee to update this policy on an annual basis.
- Undertaking training so that they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff and external agencies, where appropriate, on online safety matters.
- Ensuring safeguarding is considered in the school's approach to remote learning.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- 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.
- Reporting to the Local Academy Committee about online safety on a termly basis.

ICT technicians* will be responsible for:

- Providing technical support in the development and implementation of online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher and wider members of Ad Astra Academy Trust staff.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL/Headteacher to conduct regular light-touch reviews of this policy.

**At West View Primary School, the ICT technician role is undertaken by OneIT.*

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to, adhering to the Acceptable Use Agreement and other relevant policies.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Engaging with training to ensure that they have an awareness of online safety issues and are familiar with, and understand, the indictors that pupils may be unsafe online.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns.

Managing Online Safety

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

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

concerns about pupils' safety online. The DSL should liaise with the Police or children's social care services for support responding to harmful online sexual behaviour.

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

- Staff and Local Academy Committee members receive regular training.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Staff's knowledge and understanding regarding online safety is checked as part of the monthly safeguarding quizzes which are in place.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted on the topic of remaining safe online.

Handling Online Safety Concerns

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

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

Confidentiality will not be promised. If the decision is made to report abuse to children's social care or the Police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the Chief Executive Officer of the Trust.

Concerns regarding a pupil's online behaviour are reported to the DSL (who is also the Headteacher), who investigates concerns with relevant staff members, e.g. the SENDCO and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the Police. As a school, we avoid 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. The Headteacher/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 Headteacher/ DSL.

Cyberbullying - *please refer to our Anti-Bullying and Safeguarding Policies.*

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 e.g. homophobia/racism.

We are aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying Policy.

Child-on-Child Sexual Abuse and Harassment

Child on Child Abuse - Tees Safeguarding Children Partnerships' Procedures (teescpp.org.uk)

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff understand that this abuse can occur both in and outside of school, off and online, and remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

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

- Threatening, facilitating or encouraging sexual violence.
- Upskirting - *taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.*
- Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial, harmless or 'banter'. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

As a school, we will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking 'sides', often leading to repeat harassment. We will respond to these incidents as well as all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment, in line with the Anti-Bullying, Child-on-Child Abuse and Safeguarding Policies.

Grooming and Exploitation

What Parents Need to Know About Sexual Grooming | NSPCC

Child Exploitation - Tees Safeguarding Children Partnerships' Procedures (teescpp.org.uk)

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

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

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

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

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Child Sexual Exploitation - Tees Safeguarding Children Partnerships' Procedures (teescpp.org.uk)

Child Criminal Exploitation - Tees Safeguarding Children Partnerships' Procedures (teescpp.org.uk)

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

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

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

Radicalisation – *please refer to our PREVENT policy.*

Prevent / Channel Referral Process - Tees Safeguarding Children Partnerships' Procedures (teescpp.org.uk)

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

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

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the school's Safeguarding and PREVENT policies.

Mental Health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The Headteacher/DSL will ensure that training is available to help staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Online Hoaxes and Harmful Online Challenges

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

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

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

Prior to deciding how to respond to a harmful online challenge or hoax, the Headteacher/DSL will decide whether each proposed response is:

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

Where the Headteacher/DSL's assessment finds an online challenge to be putting pupils at risk of harm, 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 individual pupils at risk where appropriate.

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

Cyber-Crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

As a school, we will factor into our approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices - National Crime Agency which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online Safety: CPD for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online Safety: Curriculum

Online safety is embedded throughout the curriculum. Online safety teaching is always appropriate to pupils' ages and developmental stages.

As a school, we implement the 'Education for a Connected World Framework' - Education for a Connected World - GOV.UK (www.gov.uk)

Through this, pupils are taught about:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security

- Copyright and ownership

Further details about the content covered in each of the above strands can be found here: Education for a Connected World (publishing.service.gov.uk)

Relevant members of staff will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

As a school, we will endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher/DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL (or deputy) will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be 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 will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities or if a pupil makes a disclosure to a member of staff, the staff member will follow the guidelines set out in the Child Protection and Safeguarding Policy.

Use of Technology

Technology will be used during lessons. This will include the use of laptops, iPads, the intranet and emails.

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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law - Copyright, Designs and Patents Act 1988 - Consolidated (publishing.service.gov.uk)

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

Smart Technology

Whilst we recognise that the use of smart technology can have educational benefits, there are also a variety of associated risks.

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

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.

- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Staff will use all smart technology and personal technology in line with the school's Staff Behaviour Policy/Code of Conduct and Staff Acceptable Use Agreement.

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

Staff will seek to ensure that they are kept up to date with the latest devices, platforms, apps, trends and related threats.

As a school, we will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating Parents

West View Primary School will work in partnership with pupils, parents and carers to ensure pupils stay safe online at school and at home. Parents and carers will be provided with information about the school's approach to online safety and their role in protecting their children. Parents and carers will be given a copy of the Acceptable Use Agreement at the point in which their child joins the 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 and carers 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 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 and carers 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 will be raised in the following ways:

- Parents' evenings
- Dedicated training sessions
- Newsletters
- Online resources
- Promotion via social media the school website

Internet Access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

All members of the school community will be 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.

Filtering and Monitoring Online Activity

The Local Academy Committee, together with the wider Multi-Academy Trust, will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk). The Local Academy Committee will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Headteacher and ICT technicians from OneIT will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems implemented will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Headteacher. Prior to making any changes to the filtering system, ICT technicians and the Headteacher/DSL will conduct a risk assessment. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the Headteacher/DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g.

- Internet Watch Foundation - Eliminating Child Sexual Abuse Online – Internet Watch Foundation (iwf.org.uk)
- CEOP - CEOP Safety Centre
- Police

The school's network and school-owned devices will be appropriately monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network Security

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

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks directly to OneIT.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in Key Stage 2 will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords

private. Passwords will 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 will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take.

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

Emails

Access to and the use of emails will be managed in line with the Acceptable Use Agreement.

Staff will be given approved school email accounts and will only be 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 must agree to and sign the Acceptable Use Agreement – these will be sent out annually. Personal email accounts will not be permitted to be used on the school site.

Staff members and pupils will be required to block spam and junk mail, and report the matter to OneIT. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

West View Primary School will work to improve its cyber security culture and educate staff through the use of Boxphish, which provides real-world phishing simulations, training content and actionable data - Cyber Awareness Training & Phishing Simulations | Boxphish

Social Networking

The use of social media by staff and pupils will be managed in line with the Staff Behaviour Policy/Code of Conduct and Social Media Policy.

School Website

The Headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. This will be done in liaison with OneIT.

Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Acceptable Use Agreement.

For staff, the use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff Code of Conduct and Acceptable Use Agreement.

For pupils, where a school-owned device has been loaned for the purpose of assisting with school work from home, the use of the device will be managed in line with the pupil's Acceptable Use Agreement and Equipment Loan Agreement.

Remote Learning

All remote learning will be delivered in line with the school's Remote Education Plan. This specifically sets out how online safety will be considered when delivering remote education. The school's *Safeguarding Protocols for Virtual Teaching* should also be consulted.

Monitoring and Review

West View Primary School recognises that the online world is constantly changing; therefore, the DSL/Headteacher and ICT technicians conduct regular light-touch reviews of this policy to evaluate its effectiveness.

The Local Academy Committee and Headteacher (who is also the DSL) will review this policy in full on an annual basis or sooner, if needed, following any online safety incidents.

The next scheduled review date for this policy is October 2024.