Bursar Primary Academy

Online/E- Safety Policy

Co-ordinator	Sophie Follan
Policy Date	January 2025
Reviewed	September 2026
Review Date	September 2027

Online Safety Policy

Statement of Intent

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 three 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.
The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has adopted 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
•The General Data Protection Regulation (GDPR)
•Data Protection Act 2018
•DfE (2020) 'Keeping children safe in education'
•DfE (2019) 'Teaching online safety in school'
•DfE (2018) 'Searching, screening and confiscation'
•National Cyber Security Centre (2017) 'Cyber Security: SmallBusiness Guide'
•UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
•UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

This policy operates in conjunction with the following school policies:
•Allegations of Abuse Against Staff Policy
•Acceptable Use Agreement
•Child Protection and Safeguarding Policy
•Anti-Bullying Policy
•PSHE Policy, including RSE and Health Education Policy
•Staff Code of Conduct
•Behavioural Policy
•Disciplinary Policy and Procedures
•Data Protection Policy
•Device User Agreement
•Prevent Duty Policy

Roles and responsibilities

The governing board is responsible for:

Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
Reviewing this policy on an annual basis.
Ensuring their own knowledge of online safety issues is up-to-date.
Ensuring all staff undergo safeguarding and child protection training (including online safety and data protection) at induction.
Ensuring that there are appropriate filtering and monitoring systems in place.

The Headteacher is responsible for:

Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
Ensuring online safety practices are audited and evaluated.
Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.

The Online Safety Officer is responsible for:

Taking the lead responsibility for online safety in the school.
Acting as the named point of contact within the school on all online safeguarding issues.
Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
Liaising with relevant members of staff on online safety matters, e.g. the DSL, SENCO and ICT technicians.
Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
Ensuring safeguarding is considered in the school's approach to remote learning.
Ensuring appropriate referrals are made to external agencies, as required.
Staying up-to-date with current research, legislation and online trends.
Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
Ensuring all members of the school community understand the reporting procedure.
Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
Reporting to the governing board about online safety annually.
Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
Working with the Headteacher and governing board to update this policy on an annual basis.

ICT technicians are responsible for:

Providing technical support in the development and implementation of the school's online safety policies and procedures.
Implementing appropriate security measures.
Ensuring that the school's filtering and monitoring systems are updated as appropriate.
Working with the Online Safety Officer and Headteacher to conduct half-termly light-touch reviews of this policy.

All staff members are responsible for:

Taking responsibility for the security of ICT systems and electronic data they use or have access to.
Modelling good online behaviours.
Maintaining a professional level of conduct in their personal use of technology.
Having an awareness of online safety issues.
Reporting concerns in line with the school's reporting procedure.

Where relevant to their role, ensuring online safety is embedded intheir teaching of the curriculum.

Pupils are responsible for:

Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
Seeking help from school staff if they are concerned about something they or a peer has experienced online.

Reporting online safety incidents and concerns in line with the procedures within this policy.

The Computing Curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:
•Relationships, Sex, Health Education
•PSHE/ Pol-Ed
•Computing
•Discreet focused lessons (upper KS2) covering radicalisation/extremism, online grooming, online sexual abuse and county lines.

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. Or to the specific concerns of the pupils

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

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 or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

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 DSL and online safety officer 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 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged. An ask it basket will be used for further discussions

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

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

Staff Training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated annually and is delivered in line with advice from the three local safeguarding partners.

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

The DSL and any deputies 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. Online safety training is delivered to the DSL on an annual basis alongside all staff

In addition to this formal training, the DSL and any deputies receive regular online safety updates from the online safety officer 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 receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns, in line with the Safeguarding Policy.

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

Educating Parents

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:
• Parent section on website
• Awareness sessions
• Newsletters
• ClassDojo messages and stories.

Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Classroom Use
A wide range of technology is used during lessons, including but not exhaustive to the following:
• Computers
• Laptops/ Chromebooks
• Tablets
• Internet
• Email
• Cameras
• Webcams

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.

Class teachers do not sign up to any online sites without checking with the data protection officer to ensure compliance

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

Internet Access

AUP's are completed annually. EYFS' are sent home for parents to read to the child and sign. KS1&2 are explained to the children in class and signed for.

All members of the school community 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 governing board have overall responsibility but the ICT Technicians ensure the school's ICT network has appropriate filters and monitoring systems in place

The Online Safety Officer and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The Headteacher/Online Safety Officer and ICT Technicians ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The school filtering systems are monitored regularly by the ICT Technicians to ensure they remain effective and appropriate via advanced systems in place to flag up any inappropriate content/ system issues. Random spot checks take place annually to test the policies/access levels set for each school remain consistent towards the different layers of filtering for Staff, Teachers and Pupils.

Requests regarding making changes to the filtering system are directed to the Headteacher.

Prior to making any changes to the filtering system, ICT technicians and the Online Safety Officer conduct a risk assessment.

Reports of inappropriate websites or materials are made to the Online Safety Officer or ICT technicians immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the Online safety officer and ICT technicians, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
The school's network and school-owned devices are appropriately monitored.

All users of the network and school-owned devices are informed about how and why they are monitored.

Concerns identified through monitoring are reported to the Online Safety Officer who manages the situation in line with the Safeguarding Policy.
Random safeguarding checks will be carried out on the school network and school owned devices.

Network Security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.

Firewalls are switched on at all times.

ICT technicians review the firewalls on a regularly to ensure they are running correctly, and to carry out any required updates.

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

Staff members report all malware and virus attacks to ICT Helpdesk.

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. Staff should not write them down and leave visible to others

Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Office 365 passwords expire after 90 days, after which users are required to change them.

Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

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

Users log it with the ICT helpdesk 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 or otherwise mistreating the password system, the Headteacher is informed and decides the necessary action to take.

Full details of the school's network security measures can be found in the Data and E-Security Breach Prevention and Management Plan.

E-mails

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

Staff use school email for communication between staff parents/carers and pupils. The emails must remain professional in tone and content

Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant acceptable use agreement.

Personal email accounts are not permitted to be used on the school site.

Staff must protect the identities of multiple recipients by using the BCC in emails

Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians.

The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.

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

Teachers deliver lessons where they explain what a phishing email and other malicious emails might look like – these lessons include information on the following:

•How to determine whether an email address is legitimate
•The types of address a phishing email could use.

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 during lesson time.

Staff on induction are advised that their conduct on social media can have an impact on their role and reputation within the school. Building an understanding of safe and professional behaviour in line with the DFE advice, being careful about subjects discussed online.

Staff will not post inappropriate content or participate in any conversations which will be damaging to the reputation of the school.

Staff should not accept friend requests from pupils past or present under the age of 18 years old.

Staff receive training on how to use social media safely and responsibly.

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.

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

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

In the case of a critical incident staff will not make any comment on social media without the permission of senior management

If you have parents as friends on social media you should never post, comment, share any material that identifies the school, working in a school, naming pupils, parents or staff or never post, comment or share any material deemed to be offensive or persuasive (sexual, religious, racist, political etc). Doing so will result in disciplinary action or dismissal.

Use on Behalf of the School

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

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

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

The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Pupils contributions to social media sites and blogs/vlogs are moderated by the teacher before being approved.

The School Website

The Headteacher is responsible for the overall content of the school website (or directs the Website Lead) – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if prior consent is obtained. A record of this consent is kept in the front office.

Use of School-owned Devices

Some staff members are issued with the following devices to assist with their work.
Staff must sign an agreement before taking off site:
• Laptop
• Ipad

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g., tablets to use during lessons. Some devices are allocated to specific pupils for home learning. Parental agreements are signed prior to leaving site. The serial number of that device is recorded onto the agreed home use agreement and stored on the one drive in the correct folder.

School-owned devices are used in accordance with the Device User Agreement and AUP.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

All school-owned devices are password protected.

All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all school-owned devices on an annual basis to ensure there is no inappropriate material on the devices.

No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behaviour Policy.

Use of Personal Devices

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

Personal devices (including smartwatches) are not permitted to be used in the following locations:
-Classrooms during directed teaching times
-Pupils toilets
-Playground

Staff members are not permitted to use devices for texting, phone calls and personal emails during lesson time.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the discipline policy.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Headteacher/online safety officer will inform the police and action will be taken in line with the discipline policy.

The serial number and name will be recorded for the pupils who have been granted permission to use their personal device in school – The school must liaise with the parent to ensure suitable malware/anti-virus protection is installed on the device

If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office.

Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation guidance DFE

If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL and Online Safety Officer.

Visitors will be given a guest password to access the schools WIFI.

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 & PSHE curriculum
• Assemblies
• 1:1 intervention

Concerns regarding a staff member's online behaviour are reported to the headteacher and Online Safety Officer who decides on the best course of action in line with the relevant policies, e.g. Staff Code of Conduct and Disciplinary Policy and Procedures.

Concerns regarding a pupil's online behaviour are reported to the DSL and online safety officer who investigates 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. Behaviour Policy and Child Protection and Safeguarding Policy.

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

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

The Safeguarding Policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

Responding to Specific Online Safety Concerns
Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated.

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

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

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

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

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 school.

Incidents of upskirting are reported to the DSL and Online Safety Officer who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth Produced Sexual Imagery (Sexting)

Youth produced sexual 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 illegal.

All concerns regarding sexting are reported to the DSL and Online Safety Officer.

Following a report of sexting, the following process is followed:

•The DSL holds an initial review meeting with appropriate school staff
•Subsequent interviews are held with the pupils involved, if appropriate
•Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
•At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
•The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members do not view the youth produced sexual imagery unless

If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.

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

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

it is necessary to view the imagery, it will not be copied, printed or shared.

Viewing and deleting imagery is carried out in line with the Searching, Screening and Confiscation guidance.

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 responds 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/Online safety officer and dealt with in line with the Child Protection and Safeguarding Policy.

Online Hate

The school 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 policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct and Anti-Bullying Policy

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 Policy.

Remote Learning

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

All staff and pupils using video communication must:

Microsoft Teams will be used for video conferencing set up with their school email account
If another platform is used with pupils' teachers will makes sure it is age appropriate and complies with GDPR.
•Teachers and pupils will not use personal accounts
•Written consent will be sort from parents and carers and the benefits and risks will be explained clearly.

•Appropriate staff should supervise and be on hand to handle any sudden changes or upsetting developments that may occur during livestream.
•Gaining consent is essential before the recording of any live stream or video conference.
•Communicate in groups – one-to-one sessions are only carried out where necessary and must have the Headteacher's permission.
•Wear suitable clothing – this includes others in their household.
•Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
•Use appropriate language – this includes others in their household.
•Maintain the standard of behaviour expected in school.
•Use the necessary equipment and computer programs as intended.
•Not record, store, or distribute video material without permission.
•Ensure they have a stable connection to avoid disruption to lessons.
•Always remain aware that they are visible.
•Risk assessments will be completed

All staff and pupils using audio communication must:

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

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

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

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

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish downloaded, where required.

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

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

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

AI & Deep Fakes

In line with Keeping Children Safe in Education (KCSiE) 2026, the school recognises the growing role of artificial intelligence (AI) and generative AI technologies in children's online experiences. Pupils, staff and parents should be aware that AI can be used to create, alter or manipulate content, including indecent, semi-indecent or misleading images and videos commonly referred to as "deepfakes". Such content can be difficult to identify as false and may be used to bully, exploit, deceive or harm others. The school will educate pupils about the safe, responsible and ethical use of AI, including how to critically evaluate online content, recognise potential risks, report concerns and seek support. Online safety education will address the four areas of online risk (content, contact, conduct and commerce) and will include emerging risks associated with AI-generated content. Any concerns regarding the misuse of AI, deepfakes or other online technologies will be managed in line with the school's safeguarding, behaviour and child protection procedures.

The school acknowledges that safeguarding concerns may arise from AI-generated or digitally manipulated content, including deepfake images, audio and video. Where such content is suspected or identified, it will be treated as a safeguarding concern and responded to in accordance with child protection procedures and relevant statutory guidance, including KCSiE 2026.

Filtering, Monitoring and Mobile Phones

Filtering and Monitoring

The school recognises the vital role that effective filtering and monitoring systems play in safeguarding children online. In accordance with Keeping Children Safe in Education (KCSiE) 2026, the school will ensure that appropriate filtering and monitoring arrangements are in place and operate effectively across all internet-enabled devices, networks and systems used within the school. Filtering systems will be designed to limit children's exposure to inappropriate, harmful or illegal content, whilst monitoring systems will support the identification of safeguarding concerns and potential online risks. The effectiveness of filtering and monitoring arrangements will be reviewed regularly by school leaders and those responsible for safeguarding and IT provision to ensure that systems remain robust, proportionate and responsive to emerging technologies and risks.

Mobile Phones and Personal Devices

The school is committed to creating a safe, focused and disruption-free learning environment. In line with government expectations and KCSiE 2026, pupils will not have access to mobile phones or other personal internet-enabled devices during the school day. Where pupils bring mobile phones to school, these must be

switched off and stored in the school office. Any misuse of mobile phones, including taking or sharing images, accessing inappropriate content, cyberbullying or bypassing school filtering and monitoring systems, will be addressed in line with the school's behaviour, safeguarding and child protection policies.

The school will regularly communicate its approach to mobile phone use and online safety to pupils, parents and carers, ensuring all members of the school community understand their responsibilities in helping to keep children safe online.

Monitoring and Review

The school recognises that the online world is constantly changing; therefore, the online safety officer conducts half-termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and online safety officer review this policy in full on an annual basis and following any online safety incidents.

Any changes made to this policy are communicated to all members of the school community

Equal Opportunities and Inclusion Statement:

At Bursar Primary Academy, we consider all pupils to be of equal value; our pupils deserve equal access to every element of school life. We believe that they have equal opportunities to learn and work together to achieve their highest possible levels of achievement. Bursar Primary Academy is an inclusive school developing learners who thrive and flourish during their primary school career.