BIRKENHEAD
SCHOOL

Online Safety Policy

Reviewed by DSL: Graham Murdoch, October 2026
Reviewed by Governor: Nicky Thorp, September 2026
Next review: August 2027

1. Policy Introduction and Aims

The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is still constantly changing. In order to ensure that the school provides a safe environment for learning, we adhere to the following principles: The School adopts a safeguarding-first approach to online safety. Online safety concerns are treated as safeguarding concerns whenever there is potential risk of harm to a child.

Relationship with Safeguarding and Child Protection

This Online Safety Policy forms part of the School's wider safeguarding framework and should be read alongside the Safeguarding and Child Protection Policy. The School recognises that online safety is a safeguarding issue and that concerns arising from online activity may indicate abuse, exploitation, harmful sexual behaviour, bullying, radicalisation, mental health concerns or other forms of harm. Online safety concerns which present a risk of harm will be managed in accordance with safeguarding and child protection procedures.

Online safety is embedded throughout the School's safeguarding culture, curriculum, pastoral systems, staff training, behaviour expectations, filtering and monitoring arrangements and partnership work with parents and external agencies.

Recording and Management of Concerns

All online safety concerns and actions taken will be securely recorded within safeguarding systems. Records of online safety concerns, referrals and actions taken will form part of safeguarding records and be retained in accordance with safeguarding and data retention requirements.

- Online safety is an essential part of safeguarding, and the school has a duty to ensure that all students and staff are protected from potential harm online

• Online safety education is an important preparation for life. Students should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online

The purpose of the online safety policy is to:

• Safeguard and protect all members of the school's community online
• Identify approaches to educate and raise awareness of online safety throughout the community • Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
• Identify clear procedures to use when responding to online safety concerns.

The four 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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, 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 the user 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 scams

2. Policy Scope

This policy applies to all staff including teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as students and parents/carers. It applies to the whole school including the Early Years Foundation Stage. It applies to access to school systems, the internet, and the use of technology, using devices provided by the school or personal devices internet usage when connected to school WiFi.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

2.1 Links with other policies and practices

This policy links with a number of other policies, including:

• The Safeguarding and Child Protection Policy.
• KCSIE: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
• The Data Protection Policy

- Local Safeguarding Arrangements: The School will act in accordance with local safeguarding partnership arrangements and local threshold guidance.
- The Staff Code of Conduct
- Acceptable Use Agreements (AUAs) for staff and students
- The school's Behaviour Policy
- The school's Anti-Bullying Policy

3. Roles and Responsibilities

- Graham Murdoch is the Designated Safeguarding Lead (DSL) responsible for online safety
- All members of the community have important roles and responsibilities to play with regard to online safety:

3.1 The Principal & CEO

- Has overall accountability for online safety provision
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with national recommendations and requirements
- Ensures the school follows policies and practices regarding online safety (including the Acceptable Use Agreements), information security and data protection
- Ensures that online safety is embedded within the whole school curriculum, which enables all students to develop an age-appropriate understanding of online safety
- Supports the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities
- Ensures that all staff receive regular, up to date and appropriate online safety training
- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal and national support
- Receives regular reports from the DSL on online safety
- Ensures that online safety practice is audited and evaluated regularly to identify strengths and areas for improvement.

3.2 The Designated Safeguarding Lead (DSL)

- Takes lead responsibility for online safety and safeguarding, including maintaining an up-to-date understanding of filtering and monitoring systems and processes, online risks, artificial intelligence technologies, escalation procedures and the safeguarding implications of online activity. As Designated Safeguarding Lead and Deputy Head (Pastoral & Operations), the postholder also has strategic responsibility for the oversight, review and effectiveness of filtering and monitoring arrangements across the School.
- Promotes an awareness of and commitment to online safety throughout the school community • Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to students
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Monitors student internet usage, taking action where required

- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends
- Works with technical staff to ensure filtering and monitoring systems remain effective and appropriate, undertakes a formal annual review of filtering and monitoring provision, ensures records of reviews and actions taken are maintained, and reports significant findings to Governors and Senior Leadership as appropriate.
- Monitoring alerts will be reviewed in accordance with agreed safeguarding procedures. Trends, themes and patterns will be analysed termly by the DSL and reported to senior leaders and governors.
- Reports regularly to the Principal & CEO and SLT on the incident log, internet monitoring, current issues, developments in legislation etc.
- Maintains awareness of local safeguarding partnership procedures, local threshold documents and referral pathways and ensure appropriate escalation of online safety concerns.
- Provides governors with regular assurance information regarding online safety risks, incidents, trends, filtering and monitoring effectiveness and compliance with relevant statutory guidance.
- Leads the formal annual review of filtering and monitoring arrangements and ensures findings, actions and review dates are recorded and reported to senior leaders and governors.
- Undertakes a documented annual online safety risk assessment and ensures resulting actions are implemented and monitored.
- Ensures that pupil voice contributes to the ongoing development and evaluation of the School's online safety arrangements.
- Reviews online safety incidents, safeguarding records and monitoring information at least termly to identify patterns, trends, emerging risks and training needs.
- Oversees the evaluation of online safety reporting routes to ensure that students remain confident in seeking support and reporting concerns.
- Maintains awareness of emerging technologies, online platforms, artificial intelligence developments and associated safeguarding risks, ensuring that risk management strategies remain current and proportionate.

DSL Availability and Cover Arrangements

The School maintains robust cover arrangements to ensure online safety and safeguarding concerns are received, monitored and acted upon without delay whenever the DSL is unavailable. Appropriately trained Deputy DSLs provide cover, and safeguarding reporting mechanisms will always remain accessible to ensure continuity of safeguarding oversight and response.

3.3 Staff managing the technical environment

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Keep up to date with the school's online safety policy and technical information to carry out their online safety role effectively and to inform and update others as relevant
- Provide technical support to the DSL and leadership team in the implementation of online safety procedures
- Ensure that the school's filtering policy is applied and updated on a regular basis, and oversees the school's monitoring system
- Report any filtering breaches or other online safety issues to the DSL, Principal & CEO, Governors and other bodies, as appropriate

• Ensure that any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures.

3.4 All school staff

• Read, adhere to and help promote the online safety policy, Acceptable Use Agreements and other relevant school policies and guidance
• Take responsibility for the security of school systems and the data they use, or have access to
• Model safe, responsible and professional behaviours in their own use of technology
• Embed online safety in their teaching and other school activities
• Supervise, guide and monitor students carefully when engaged in activities involving online technology (including co-curricular and extended school activities if relevant)
• Have an up-to-date awareness of a range of online safety issues and how they may be experienced by the children in their care
• Identify online safety concerns and take appropriate action by reporting to the DSL
• Know when and how to escalate online safety issues

Staff will exercise professional curiosity where online activity, behaviour, attendance, relationships or presentation raises safeguarding concerns.

• Take personal responsibility for professional development in this area.

3.5 Students (at a level appropriate to their individual age, ability and vulnerabilities)

• Engage in age-appropriate online safety education opportunities
• Read and adhere to the school Acceptable Use Agreements
• Respect the feelings and rights of others both on and offline, in and out of school • Take responsibility for keeping themselves and others safe online
• Report to a trusted adult, if there is a concern online.

3.6 Parents and carers

• Read the school Acceptable Use Agreements and encourage their children to adhere to them
• Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home • Model safe and appropriate use of technology and social media
• Identify changes in behaviour that could indicate that their child is at risk of harm online
• Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
• Use school systems, such as learning platforms, and other network resources, safely and appropriately
• Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

3.7 External groups

• Any external individual/organisation must sign an Acceptable Use Agreement prior to being given individual access to the school network.

3.8 Governors

Governors recognise online safety as a safeguarding responsibility and provide strategic oversight of the School's online safety arrangements.

Governors will:

- Ensure that the School meets statutory safeguarding and online safety requirements.
- Challenge and support leaders regarding the effectiveness of online safety arrangements and risk management.
- Ensure that sufficient resources are available to maintain effective safeguarding, filtering and monitoring arrangements.
- Review assurance information relating to online safety incidents, trends, safeguarding concerns, training, filtering and monitoring effectiveness and compliance with relevant statutory guidance.
- Review the findings of annual online safety risk assessments and filtering and monitoring reviews.
- Seek assurance that pupils know how to report concerns and that reporting systems are effective and accessible.
- Monitor the impact and effectiveness of the School's online safety curriculum.
- Review this policy and wider online safety arrangements at least annually.

Governors will maintain oversight of compliance with the DfE Filtering and Monitoring Standards and ensure that online safety remains a standing safeguarding consideration within governance discussions throughout the academic year.

4. Education and Engagement

4.1 Education and engagement with students

The school curriculum includes age-appropriate lessons and activities on online safety for all students, intended to raise awareness, build resilience, and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety across the curriculum, including the Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home
- Reinforcing online safety messages whenever technology or the internet is in use
- Ensuring that the needs of students considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum
- Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching students to be critically aware of what they see online and shown how to validate information before accepting its accuracy
- Teaching students to respect and adhere to principles of academic integrity. This will include understanding the importance of producing their own independent work, being transparent and honest about any use of source material or generative applications, respecting copyright and using appropriate referencing conventions
- Supporting students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making

The school will support students to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:

- Discussing the AUA and its implications, and reinforcing the principles via display, classroom discussion etc.
- Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Teaching students to understand emerging online risks, including generative artificial intelligence, deepfakes, misinformation, disinformation, financially motivated scams, online sexual harassment and exploitative online behaviours.
- Promoting a culture of respectful online behaviour and challenging misogyny, misandry, discrimination and harmful online attitudes. This includes online sexual extortion (sextortion), coercive image-based abuse, money mule recruitment, cryptocurrency scams, financial exploitation and exposure to violent or weapon-related content.
- Recognising positive use of technology by students.

Students may report concerns to trusted staff, Form Tutors, the DSL, Deputy DSLs, through the School safeguarding email address safeguarding@birkenheadschool.co.uk, Childline, CEOP and Report Remove. Reporting routes are well publicised, accessible and developmentally appropriate. Students will be reassured that concerns are taken seriously, responded to promptly and managed sensitively.

4.2 Training and engagement with staff

The school will:

- Provide and discuss the Online Safety Policy and staff Acceptable Use Agreement with all members of staff as part of induction
  All staff, including those who do not work directly with children, will receive safeguarding induction and be required to read at least Part One of KCSIE together with Annex A where appropriate to their role.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring,
- Make staff aware that school systems are monitored and activity can be traced to individual users through the Smoothwall Monitoring system. Staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the school community.

4.3 Awareness and engagement with parents and carers

Parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings
- Informing parents about what the school asks students to do online, and who they will be interacting with
- Drawing parents' attention to the school online safety policy and expectations in newsletters and on the website
- Requiring parents to read the student Acceptable Use Agreement and discuss its implications with their children.

Online safety risk assessments will take account of safeguarding intelligence, pupil voice, behaviour data, filtering and monitoring reports, local safeguarding partnership information and emerging national risks.

4.4 Pupil Voice

The School recognises the importance of understanding pupils' online experiences and listening to their views regarding online safety. The School will:

- Seek pupil views regarding online safety through surveys, discussions, pastoral systems, school council activity and safeguarding reviews.
- Encourage pupils to contribute to the development of online safety education and awareness initiatives.
- Monitor feedback regarding online risks, reporting systems and support mechanisms.
- Use pupil feedback to inform policy development, curriculum planning and safeguarding practice.

Pupil voice will be considered alongside safeguarding intelligence, incident records and emerging national guidance when reviewing online safety provision.

5. Reducing Online Risks

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

- Regularly review the methods used to identify, assess and minimise online risks
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- Ensure, through online safety education and the school AUAs, that students know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networks are used or not.

Online safety concerns will be considered within the wider context of extra-familial harm, including peer groups, social media platforms, gaming environments, community contexts and online spaces where abuse, exploitation or harmful influence may occur.

Staff will understand local Family Help pathways, threshold guidance and referral processes, including when concerns should be escalated from internal support to Family Help services, Children's Social Care or the Police.

Vulnerable Pupils: Additional protections may be required for SEND pupils, children with social workers, looked after and previously looked after children, young carers and vulnerable learners.

Digital Platform and Technology Assessment

Before introducing new digital platforms, applications, software, artificial intelligence tools, online services or internet-enabled technologies, the School will undertake appropriate due diligence and risk assessment.

Consideration will include: safeguarding implications; age appropriateness; data protection and privacy; cyber security; moderation and reporting functions; filtering and monitoring implications; accessibility requirements; educational benefit. Additional safeguards may be implemented where risks are identified.

6. Safer Use of Technology

6.1 Classroom Use

The school uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites • Learning platforms
- Cloud services and storage
- Email and messaging
- Games consoles and other game based technologies
- Digital cameras, web cams and video cameras
- Virtual reality headsets
- Artificial intelligence

Supervision of students will be appropriate to their age and ability. All devices should be used in accordance with the school's AUAs and with appropriate safety and security measures in place. Members of staff should always thoroughly check websites, tools and apps for suitability before use in the classroom or recommending for use at home. Staff and students should consider copyright law and principles of academic integrity before using internet-derived materials (and where appropriate comply with licence terms and/or acknowledge the source of information).

1.2 6.2 Filtering and Monitoring

The School operates on a single network, with a connection to the internet that is managed by a firewall, filter and monitoring systems. This system inspects internet traffic to block malware and many other threats. The system also blocks access to and from a number of harmful and malicious websites. The firewall access rules are managed centrally by the IT team. The system also provides in depth monitoring, analysis and reporting on activity by users on all school-managed devices. All devices used by students are connected to the School wi-fi and bound by the same filtering and monitoring. Students know not to use 3G, 4G or 5G access to circumnavigate the filtering and monitoring systems.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students: effective classroom management and regular education about safe and responsible use is essential.

All users are informed that use of school systems is monitored and that all monitoring is in line with data protection, human rights and privacy legislation.

The effectiveness of the School's filtering and monitoring arrangements will be formally reviewed at least annually by the Designated Safeguarding Lead in conjunction with the I.T. Manager. The annual review will assess compliance with the DfE Filtering and Monitoring Standards, evaluate existing controls, review internet-connected devices, consider incidents and emerging risks, record findings and actions, and be reported to the Senior Leadership Team and Governors as appropriate.
The School will implement the DfE Filtering and Monitoring Standards by assigning clear responsibilities, maintaining effective monitoring strategies, reviewing provision regularly, and ensuring harmful content is blocked without unreasonably restricting teaching and learning. Records of filtering and monitoring reviews, testing activities, device checks, identified risks, actions taken and follow-up evaluations will be maintained securely. Reviews will include checks on filtering and monitoring effectiveness across all relevant internet-connected devices, systems and locations used by students and staff.

The DSL will undertake a termly review of filtering and monitoring incidents and reports to identify emerging themes, patterns of behaviour, safeguarding concerns and areas requiring intervention, training or curriculum development. Significant concerns, trends and actions taken will be reported through safeguarding reporting arrangements to senior leaders and governors as appropriate.

6.3 Dealing with Filtering Breaches

The school has a clear procedure for reporting filtering breaches:

- If students discover unsuitable sites, they will be required to alert a member of staff immediately
- The member of staff will report the concern (including the URL of the site if possible) to the DSL
- The breach will be recorded and escalated as appropriate
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as Internet Watch Foundation (IWF), the Police or Child Exploitation and Online Protection (CEOP).

6.4 Managing Personal Data Online

Personal data will be collected, processed, stored and transferred in accordance with the UK GDPR, the Data Protection Act 2018 and other relevant data protection legislation and the School's Privacy Notices. Full information can be found in the school's Data Protection Policy.

The School recognises that cyber security forms part of its wider safeguarding responsibilities. The School will have regard to the Department for Education Cyber Security Standards for Schools and Colleges and will implement proportionate measures to protect systems, data and users from cyber risks that may impact safeguarding, education or business continuity.

6.5 Artificial intelligence (AI)

- Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.
- We recognise that AI has many uses to help pupils learn, but it may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. We will treat any use of AI to bully pupils very seriously, in line with our anti-bullying policy.

Staff should also consider safeguarding, data protection, intellectual property and academic integrity implications when using generative AI technologies. AI-generated content may increase risks relating to misinformation, disinformation, impersonation, exploitation, harassment, bullying and harmful imagery.

Staff should be aware of the risks of using AI tools while they are still being developed and should monitor where new AI tools are being used by students and report these to the DSL.

The DSL will complete a documented annual online safety risk assessment. The assessment will consider emerging technologies, AI tools, deepfakes, misinformation, online exploitation, harmful content, vulnerable pupils, technical controls, staff training requirements and curriculum priorities. Findings will inform safeguarding strategy, staff training, curriculum development, filtering and monitoring arrangements and governor assurance reporting.

7. Social Media

7.1 Expectations

The term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger. All members of the school community are expected to engage in social media in a positive, safe and responsible manner at all times.

7.2 Staff Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites is discussed with all members of staff as part of staff induction and is revisited and communicated via regular staff training opportunities. Safe and professional behaviour is outlined for all members of staff as part of the staff Code of Conduct, staff Acceptable Use Agreement

7.3 Students' Personal Use of Social Media

Safe and appropriate use of social media will be taught to students as part of online safety education, via age-appropriate sites and resources. The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age. The school will control student access to social media whilst using school-provided devices and systems on site.

The use of social media during school hours for personal use is not permitted. Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities. Any concerns regarding students' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

8. Use of Personal Devices and Mobile Phones

Birkenhead School is a mobile phone-free school for all students in Years 7 to 11. The School believes that reducing access to mobile phones during the school day supports student wellbeing, concentration, social interaction, behaviour and safeguarding. Students in Years 7 to 11 may bring a mobile phone to school for travel or safety reasons. However, mobile phones must not be accessible during the school day.

All students in Years 7 to 11 who bring a mobile phone to school must hand it in at morning registration to their Form Tutor. Students arriving after registration must hand their mobile phone to The Lodge immediately on arrival.

Mobile phones will be securely stored and returned at the end of the school day. Students must not retain a mobile phone on their person during the school day, access or attempt to use a mobile phone, use mobile data to bypass school filtering and monitoring systems, or use another student's device to access mobile phone functions. Failure to comply may result in confiscation and disciplinary action. Sixth Form students may carry and use mobile phones only in accordance with Sixth Form expectations and school rules.

8.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-Bullying, Behaviour, BYOD and Mobile Phone, and Safeguarding and Child Protection.
- The School's mobile phone-free arrangements form part of its wider safeguarding and online safety strategy and help reduce distraction, cyberbullying, harmful online interactions and unauthorised recording during the school day.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms and toilets.
- The sending of abusive or inappropriate messages/content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt according to the behaviour policy
- All members of the community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school behaviour or Safeguarding and Child Protection policies.

8.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that the use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as:
  Code of Conduct, Safeguarding and Child Protection, Data Security and Acceptable Use Agreements.
- Personal digital recording devices must not be used for taking, editing, or transferring images or videos of students (other than a member of staff's own children) unless permission has been sought and agreed for such.

- Staff working with Early Years' children must ensure that personal mobile phones and technological devices are out of sight and reach of children at all times and on silent if in ear shot.
- Staff working with Early Years' children are not permitted to use their mobile phones in the presence of EYFS children except when necessary for school business during an educational visit.

8.3 Students' Use of Personal Devices and Mobile Phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences
- Students' personal devices are expected to be kept securely
- If a student needs to contact their parents or carers they should do so via the reception staff
- Parents are advised to contact their child via reception staff during school hours
- Mobile phones or personal devices will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's grade in that examination or all examinations being nullified.
- If a student breaches the school policy, the phone or device will be confiscated and will be held in a secure place for 24 hours or over the weekend if on a Friday

Searches for and of mobile phone or personal devices will only be carried out in accordance with the relevant government guidance. Schools are not required to inform parents before a search takes place or to gain consent for a search for a prohibited item, or item which a member of staff reasonably suspects has been or is likely to be used to commit an offence or to cause personal injury or damage to the property of any person. A search without consent will only be conducted by a member of staff of the same sex as the student being searched and authorised by the DSL. There will also be a member of staff acting as a witness. A student's possessions will only be searched in the presence of the student and a witness.

Where the person conducting the search finds an electronic device that is prohibited by the school rules or that they reasonably suspect has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so. They may also delete data or files if they think there is a good reason to do so, unless they are going to give the device to the police.

If there is a suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation. The confiscation and searching of a phone or other digital device will normally be carried out in consultation with a senior member of staff.

See Searching, screening and confiscation: Advice for headteachers, school staff and governing bodies DfE September 2022

8.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Agreement and other associated policies, such as Anti-Bullying and Safeguarding and Child Protection policies
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of school policy.

9. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, the making, possessing and sharing of nudes and semi-nudes, including AI-generated sexual imagery, self-generated images of sexual abuse as a result of online grooming, cyberbullying and illegal content
- • All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Network Manager or Safeguarding Governor.
- Where there is suspicion that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised.

Incidents involving child-on-child abuse, harmful sexual behaviour, online sexual harassment, coercion, nudes and semi-nudes including AI-generated imagery, discriminatory bullying, misogyny, misandry or online exploitation will be managed in accordance with the Safeguarding and Child Protection Policy.

Students will be reminded of reporting routes including the DSL, CEOP, Childline and Report Remove. The School adopts a safeguarding-first approach to online safety. Any online safety concern presenting a potential risk of harm to a child will be treated and managed as a safeguarding concern in accordance with the Safeguarding and Child Protection Policy.

Recording and Management of Concerns:

All online safety concerns and actions taken will be securely recorded within safeguarding systems. Records of online safety concerns, referrals and actions taken will form part of safeguarding records and be retained in accordance with safeguarding and data retention requirements.

9.1. Concerns about Students' Welfare

- The DSL will be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern
- The DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies

9.1a Multi-Agency Working

Where an online safety concern indicates that a child may be suffering, or is at risk of suffering, significant harm, exploitation or abuse, the School will follow safeguarding and child protection procedures and work in partnership with relevant agencies.

The DSL or Deputy DSL will liaise with the Wirral Safeguarding Children Partnership, Children's Social Care, the Integrated Front Door, the Police, health professionals and other safeguarding partners as appropriate. Referrals will be made in accordance with local threshold guidance and safeguarding partnership procedures.

Online safety concerns involving child-on-child abuse, harmful sexual behaviour, exploitation, radicalisation, serious violence, criminal exploitation, sexual exploitation, AI-generated sexual imagery or other safeguarding risks will be managed through the School's safeguarding procedures and multi-agency arrangements where required. The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

9.2. Misuse

- Complaints about IT misuse by students will be dealt with by a senior member of staff under the relevant policies and procedures and according to the nature of the complaint.
- Any complaint about staff misuse will be referred to the DSL.
- Students and parents are informed of the school's complaints procedure.

10. Monitoring and Review

The school will monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice. The School will seek and consider pupil voice when reviewing online safety provision, curriculum content, reporting routes and emerging online risks.

The policy framework will be reviewed by the Governors at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place.

As part of the annual review process, leaders will consider: safeguarding incident data; pupil voice; parent feedback; staff feedback; filtering and monitoring reviews; technological developments; artificial intelligence developments; local safeguarding intelligence; national guidance and legislation. Findings will inform policy updates, curriculum planning, staff training priorities, safeguarding strategy and governor assurance reporting.

11. Useful links and sources of advice

11.1 Guidance and resources

- Teaching Online Safety in School (DfE)
- Education for a Connected World (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Harmful online challenges and online hoaxes (DfE)
- Cyberbullying: understand, prevent and respond (Childnet)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Self-generated child sexual abuse (IWF)
- Meeting digital and technology standards in schools and colleges March 2022 (DfE)
- Generative artificial intelligence in education (DfE)

11.2 National Organisations

• Action Fraud: www.actionfraud.police.uk • CEOP:
www.thinkuknow.co.uk
www.ceop.police.uk •
Childnet: www.childnet.com
• Get Safe Online: www.getsafeonline.org
• Internet Matters: www.internetmatters.org
• Internet Watch Foundation (IWF): www.iwf.org.uk
• Lucy Faithfull Foundation: www.lucyfaithfull.org
• NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
• The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
• UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline Telephone helpline: 0844 381 4772

Appendix 1: Remote Learning

Following the COVID-19 outbreak in 2020, the School moved to Remote Learning for the majority of students during periods of national lockdown. Now, Remote Learning continues to be a managed part of the curriculum, either as a means of providing support for individual students in specific circumstances, or as part of a more flexible and diverse educational offer which the school will continue to develop and enhance over time.

The school is committed to ensuring that online safety standards are maintained in the delivery of Remote Learning. Alongside the provisions in the Safeguarding and Child Protection Policy and Online Safety Policy, Staff Code of Conduct and Acceptable Use Agreements for staff and students, the guidelines below must be followed.

Providing a safe system

For the purposes of Remote Learning, the primary platforms used are:

Microsoft Teams
Firefly

The platforms are restricted to School users only and permissioned accordingly. Other platforms may be used at times for specific purposes. The online safety implications of any platform are carefully considered before use, and will be a key consideration in any decisions on configuration.

Any activity involving non-School users (e.g. visiting speakers or students from other schools) will be risk assessed. Virtual visiting speakers are vetted and supervised in the same way as they would be if they were coming onto the school site to deliver their material.

Some live online sessions are recorded for safeguarding purposes (as set out below). When a recording is made, access is restricted to participants and the IT Administrator. Access may be granted to others in the event of a complaint, formal investigation, or legal request (this would be carried out under the standard School policies). Further distribution is strictly prohibited. Recordings will be deleted after 12 months.

Formats for remote learning
There is a wide range of formats for remote learning, including:
• Posting activities for students at regular intervals, with students posting responses
• Providing recorded material in the form of podcasts or video tutorials
• Directing students to web-based resources and activities they can engage with on or offline, e.g., PurpleMash
• Interactive/live teaching in real time

Teachers will select the most appropriate format depending on a number of factors, including the age of the students, size of the group, nature of the activity, and the degree of support required; and taking into account the need to provide a variety of learning experiences within a lesson, across the school day/week and through a scheme of work.

Live online teaching
Interaction with a teacher is an important part of the learning process, and whilst online contact cannot replicate face to face contact, live sessions are particularly helpful as they allow contemporaneous communication, with students able to respond to staff questions – and vice versa. Live contact is also an important part of pastoral support and gives students the opportunity to interact with peers and maintain important social connections. However, it should be remembered that live online teaching remains 'one tool in the box' and, for the reasons set out above, it should be balanced alongside learning opportunities in a range of other formats. In order to safeguard both students and staff, live online sessions must be conducted following the protocols set out below.

For staff:
• Only use school approved platforms; do not use social media in communicating with students • Keep a record/log of live online lessons – date and time, attendance, what was covered, any incidents. Any serious incidents should be reported in the usual manner depending on the nature of the issue

- Maintain professional conduct during live streaming – dress appropriately, consider your surroundings (background, other household members who may come into view etc.) and blur if necessary, and remember that your microphone may be on
- Maintain the same boundaries and insist on the same standard of behaviour as in a school setting. Make specific protocols clear at the outset, e.g. muting of microphones at appropriate times, use of supervised chat only, etc.
- The DSL must be advised in advance of any 1:1 sessions. All 1:1 teaching sessions must be recorded on Microsoft Teams. Support and pastoral 1:1 sessions should be recorded on Teams unless the professional judgement of the member of staff is that this would be inappropriate, or the student is unhappy about a recording being made, in which case it is acceptable for detailed notes to be kept instead. Distribution of the recording beyond participants who have automatic access is strictly prohibited.

For students:

- Always log on through your School account and use your School email for school business
- School platforms may only be used for school business. Do not set up or engage in any activity which is not connected to school business and endorsed by your teachers
- Do not make recordings, take screenshots/screengrabs or photographs, or store or distribute footage of teachers or other students
- Be aware that some live online sessions may be recorded by the teacher
- Dress appropriately for online lessons
- Ensure that you have a safe and appropriate place to participate from. Blur your background if necessary
- Follow the school rules for conduct during online lessons as if you were in school
- Do not undermine in any way the technology used to offer video lessons
- If you have concerns about online safety, or if you feel you are being bullied, talk to someone you trust
- There are also external reporting routes you can use: Childline – for support
- CEOP – to make a report about online abuse
- UK Safer Internet Centre – to report and remove harmful online content
- https://reportharmfulcontent.com/

It is the responsibility of parents to ensure that students are monitored in their use of technology for Remote Learning as they would ordinarily do when their children are using technology at home. While students are working from home they are connected to their home broadband so their traffic doesn't go through the School firewall – parents will therefore need to ensure that age-appropriate filtering or safe search is enabled at home.

Further information on how to set this up appropriately can be found via Safer Internet: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/parental-controls-offered-yourhome-internet-provider and here: https://www.internetmatters.org/parental-controls/

- Communication during online learning is between student and teacher. Parents should communicate with staff in the usual manner, via school email or telephone
- Parents with queries about Remote Learning should contact their child's class teacher or tutor. Concerns related to safeguarding, child protection or online safety should be referred to the DSL