Online Safety Policy

For review October 2027

Contents

	Pg. No
Statement of intent	3
Context and rationale	3
Development/monitoring/review of this policy	5
Legal framework	6
Relevant Non-statutory guidance	7
The Online Safety Working Group	8
Governors	8
Headteacher and senior leaders	9
The DSL	9
DSL and E-Safety Lead	9
Network manager/technical staff	10
Teaching and support staff	10
Pupils	11
Parents and carers	12
Training and induction	12
Managing online safety	12
Handling online safety concerns	12
Cyberbullying	13
Child on child abuse	13
Grooming and exploitation	14
Child sexual exploitation (CSE) and child criminal exploitation (CCE)	15
Radicalisation	15
Mental health	15
Online hoaxes and harmful online challenges	16
Cyber-crime	17
Online safety and the curriculum	18
Use of technology in the classroom	20
Use of smart technology	20
Educating parents	20
Internet access	21
Filtering and monitoring online activity	21
Network security	22
Emails	22
Social networking	23
Personal use	23
Use on behalf of the school	23
The school website	23
Use of devices	24
School-owned devices	24
Personal devices	24
Remote learning	24
Appendices	25
Appendix A - Online harms and risks – curriculum coverage	
How to navigate the internet and manage information	
Wellbeing	
Potential issues arising	31

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors and guests) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where permitted).

Statement of intent

Rhyddings 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, staff and stakeholders.

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 of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

• Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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

Context and rationale

At Rhyddings we fully recognise the responsibilities for Child Protection and safeguarding:

• The Child Protection and Safeguarding Policy reflects the values of the 'Rhyddings Way'.

o Respect: Respect for one another and the school community

o Honesty: Be honest with staff, pupils and ourselves

o Yours: Take ownership of the school

o Democracy: Always listen to other people's opinions.

o Determination: Keep going when things get tough

o Inspire: Inspire others and set a good example

o Neighbourly: Be helpful to one another

o Generous: Give something extra to our learning and around school

o Supportive: Provide encouragement to those who need it.

We believe that:

• Children and young people should never experience abuse of any kind

• Children should be able to use the internet for education and personal development; however, safeguards need to be in place to ensure they are kept safe at all times.

All members of staff at Rhyddings have a crucial role to play in helping identify welfare concerns and indicators of possible abuse or neglect, at an early stage: referring those concerns to the appropriate organisation/ body (DSL), contributing to the assessment of a child's needs and were appropriate to on-going action to meet those needs of the child.

Online Safety Policy

E-safety at Rhyddings is supported in a holistic approach to ensure the assessments provide additional support for families too. At Rhyddings we support all pupils through internal early help services central to the pastoral support, YNOT, NEST, MHIST, and additional referrals through behaviour / 'hub' sessions offer early targeted interventions. Child Protection and Safeguarding is the responsibility of all adults and especially those working with children. Safeguarding always remains our main priority at Rhyddings.

Rhyddings fully recognises the contribution we can make to protect children from harm and to support and promote the welfare of all children who are pupils at our school. This policy applies to all stakeholders; this includes pupils, staff, parents, governors, volunteers, placement pupils and visitors. This policy will give clear direction to all stakeholders about expectations and our legal and moral responsibility to safeguard and promote the welfare of all children at our school.

Rhyddings is committed to safeguarding and promoting the physical, mental and emotional welfare of every pupil. We implement a whole-school preventative approach to managing safeguarding concerns, ensuring that the wellbeing of pupils is at the forefront of all action taken. We recognise that no single professional can have a full picture of a child's needs and circumstances. If children and families are to receive the right help at the right time, everyone who comes into contact with them has a role to play in identifying concerns, sharing information and taking prompt action.

This policy sets out a clear and consistent framework for delivering this promise, in line with safeguarding legislation and statutory guidance. It will be achieved by:

• Ensuring that members of the governing board, the headteacher, staff and all stakeholders understand their responsibilities under safeguarding legislation and statutory guidance, are alert to the signs of child abuse, and know to refer concerns to the DSL. In addition, to ensure that staff are aware that anyone can make a referral and understand professional challenge.

• Teaching pupils how to keep safe and to recognise behaviours that are unacceptable.

• Identifying and making provision for any pupil that has been subject to, or is at risk of, abuse, neglect, or exploitation.

• Creating a culture of safer recruitment by adopting procedures that help deter, reject or identify people who might pose a risk to children.

• Endeavour to provide a safe and welcoming environment where children are respected and valued; where the voice of the child is listened to and is paramount.

• Where it is believed that a child is at risk of or is suffering significant harm, the school will follow the procedures set out by our local Safeguarding Children Partnership arrangements. https://panlancashirescb.proceduresonline.com/chapters/contents.html

Development/monitoring/review of this policy

This Online Safety Policy has been developed by the Online Safety Working Group made up of:

• Headteacher/senior leaders

• Online safety officer/coordinator

• Staff – including practitioners/support staff/technical staff

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Rhyddings recognises that the online world is constantly changing; therefore, the DSL/Headteacher conducts regular light-touch reviews of this policy to evaluate its effectiveness.

The Online Safety Working Group and DSL review this policy in full on an annual basis and following any online safety incidents.

The school will monitor the impact of the policy using:

▪ Logs of reported incidents

▪ Monitoring logs of internet activity (including sites visited)

▪ Internal monitoring data for network activity- (Lightspeed, Sophos Central and Impero) further internal monitoring is completed from the LET Education Trust.

▪ Surveys/questionnaires of:

o Pupils

o Parents and Carers

o Staff

The next scheduled review date for this policy is September 2026.

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

Definitions

• ICT facilities:

o All facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service.

• Users:

o Anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

• Personal use:

o Any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.

• Authorised personnel:

o Employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

• Materials:

o Files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

Legal framework

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

• The UK General Data Protection Regulation (UK GDPR)

• Section 175 of the Education Act 2002

• Data Protection Act 2018

• DfE (2021) 'Harmful online challenges and online hoaxes'

• DfE (2026) 'Keeping children safe in education (KCSIE)'

• Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and

young people’

• DfE (2019) ‘Teaching online safety in school’

• UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’

• Working Together to Safeguard Children 2026

• Keeping Children Safe in Education, September 2026

• Guidance for Safer Working Practice 2022

• The Children Act 1989 & 2004

• Counter-Terrorism and Security Act 2015

• PACE Code C 2019

• Female Genital Mutilation Act 2003

• Sexual Offences Act 2003

• Equality Act 2010

• Domestic Abuse Act 2021

• Marriage and Civil Partnership Act 2022

• Online Safety Act 2023

Relevant Non-statutory guidance

• DfE (2015) ‘What to do if you’re worried a child is being abused’

• DfE (2017) ‘Child sexual exploitation’

• DfE (2018) ‘Information sharing’

• DfE (2020) 'Governance handbook'

• UKCIS (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’

• DfE (2022) ‘Recruit teachers from overseas’

• DfE (2022) 'Working together to improve school attendance'

• DfE (2022) 'Searching, Screening and Confiscation'

• DfE (2024) 'Meeting digital and technology standards in schools and colleges'

This policy operates in conjunction with the following school policies:

• Antibullying Policy

• Mobile phone and Device policy

• Health and Safety Policy

• Remote Learning Policy (including online lessons)

• Behaviour for Learning procedure

• Data Protection Policy

• Safeguarding and Child Protection Policy

• Privacy notice
• Prevent Duty Statement and Policy
• The use of social network sites and other forms of social media
• Acceptable ICT user agreement
• Disciplinary and dismissal Policy
• Relationships and Sex Policy

Roles and responsibilities of The Online Safety Working Group

The Online Safety Working Group is responsible for:
• Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
• Ensuring the DSL's remit covers online safety.
• Reviewing this policy 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, at induction.
• Ensuring that there are appropriate filtering and monitoring systems in place.
• Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
• Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of online safety governor to include:
• Regular meetings with the online safety coordinator/officer
• Regular monitoring of online safety incident logs
• Regular monitoring of filtering change control logs and monitoring of filtering logs (where possible)
• Reporting to relevant governors/sub-committee/meeting.

Headteacher and senior leaders

The Headteacher and senior leaders are responsible for:

• The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety may be delegated to the DSL.

• The headteacher and (at least) one other member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

• The headteacher/senior leaders are responsible for ensuring that the online safety/e-safety coordinator/officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

• The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

• The headteacher/senior leaders will receive regular monitoring reports from the online safety/E-safety coordinator/officer or DSL.

The DSL

The DSL is responsible for:

• Taking the lead along with the E-Safety Lead for online safety in the school.

• Acting as the named point of contact within the school on all online safeguarding issues.

• Ensuring appropriate referrals are made to external agencies, as required.

• 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.

DSL and E-Safety Lead

The DSL and E-Safety Lead are responsible for:

• 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 SENDCO and ICT Technician.
• 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.
• Keeping 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.

Network manager/technical staff

The network manager/technical staff is responsible for ensuring that:
• The school technical infrastructure is secure and is not open to misuse or malicious attack.
• The school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy/guidance that may apply.
• Users may only access the networks and devices through a properly enforced password protection policy.
• They keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant online safety policy documentation.
• The use of the network/internet/learning platform/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the senior leader, online safety coordinator/officer for investigation/action/sanction.
• Monitoring software/systems are implemented and updated regularly.
• Web filtering is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Teaching and support staff

These individuals are responsible for ensuring that:
• They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
• They have read, understood and signed the staff Acceptable Use Agreement.
• They report any suspected misuse or problem to the headteacher/senior leader online safety/E-safety coordinator/officer, DSL for investigation/action.
• All digital communications with pupils/parents and carers should be on a professional level and only carried out using official school systems.

• Online safety issues are embedded in all aspects of the curriculum and other activities.
• Pupils understand and follow the online safety and acceptable use agreements.
• Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• They monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
• In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and those processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

These individuals:

• Are responsible for using the school digital technology systems in accordance with the school expectations (this includes personal devices)
• Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online bullying
• Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through parents'/carers' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

• Digital and video images taken at school events
• Access to parents'/carers' sections of the website, school app and online pupil records

• Their children's personal devices in school.

Training and induction

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. 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.

Staff are trained and given refresher courses annually in the use of the monitoring and reporting software and procedures involved with:

• CPOMS (Reporting)

• Impero (E-Safety Lead does training annual) (Monitoring)

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 the E safety officer/ leader, deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

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

• Staff receive regular training.

• Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.

• Online safety is integrated into learning throughout the curriculum, most notably through the Computer Science curriculum and the PSHE Education 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 Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, Mr Williams (via CPOMS Staff Safe), who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Headteacher, it is reported to the Chair of Governors and the LET Education Trust CEO, Mr Campbell.

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

• Where there is a concern that illegal activity has taken place, the Headteacher/DSL contacts the Police.

All online safety incidents are recorded by all staff on CPOMS and the school's response are recorded by the DSL.

Cyberbullying

Cyberbullying can include 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.

• Menacing or upsetting responses to someone in a chatroom.

• Unpleasant messages sent via instant messaging.

• Unpleasant or defamatory information posted to blogs, personal websites, and social networking sites, e.g. Facebook.

• 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 abuse

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will 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.

• Up skirting, i.e., 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.

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.
The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether 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.

Grooming and exploitation

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, including the following:
• The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
• The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
• The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
• Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
• 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 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.
• 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)

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

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 the Prevent Duty 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 Prevent Duty Policy.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g., low self-esteem and suicidal ideation.

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 DSL and E-Safety Lead will ensure that training is available to help ensure that 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. Concerns about the mental health of a pupil will be dealt with in line with the safeguarding policy.

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 them 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 Headteacher/DSL will consult with the LET Education Trust/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.
- 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 DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g., those within a particular age range that is directly affected or even to individual children at risk where appropriate.
The 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:
1. 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.
2. 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.
The school will factor into its 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 programme, 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 Headteacher, DSL, E-Safety Lead along with curriculum leads will ensure that pupils are taught throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g., the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

Online safety and the curriculum

At Rhyddings online safety is embedded throughout the curriculum; however, it is particularly addressed in the Computing curriculum and the Personal, Social, Health and Economic Education curriculum, and in reference to the UKCIS document, 'Education for a Connected World – 2021 edition'.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of technology.

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. 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.
- What healthy and respectful relationships, including friendships, look like.
- Body confidence and self-esteem.
- Consent, e.g., with relation to the sharing of indecent imagery or online coercion to perform inappropriate or sexual acts.
- Acceptable and unacceptable online behaviour.
- How to identify online risks.
- How and when to seek support.
- How to identify when something is deliberately deceitful or harmful.
- How to recognise when something they are being asked to do puts them at risk or is age inappropriate.

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

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 Looked After Children. 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.

The school endeavours to take a more personalised and contextualised approach to teaching about online safety for children identified as more susceptible, and in response to instances of harmful online behaviour from pupils.

The school subscribes to the PSHE Association and all class teachers have access to these teaching resources. Class teachers review any other 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 PSHE Lead decide when it is appropriate to invite external groups into school and ensure the visitors selected, and the content, are appropriate.
Before conducting a lesson or activity on online safety, the class teacher considers 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 class teacher may seek advice from the safeguarding team on how to best support any pupil who they feel 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 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, they will make a report in line with the Child Protection and Safeguarding Policy.

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

Use of technology in the classroom

A wide range of technology is used during lessons, including but not limited to the following:

- Laptops/Desktop Computers
- Tablets
- Intranet
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

Use of smart technology

Staff will use all smart technology and personal technology in line with the school's staff handbook. Pupils will not be permitted to use personal smart devices or any other personal technology whilst on the school premises. Pupils will be educated on the acceptable and appropriate use of personal devices through the Computing curriculum and the PSHE Education curriculum. The school will also hold assemblies, where appropriate, which address issues related to the use of smart technology, and outlining the importance of using smart technology in an appropriate manner.

Where it is deemed necessary, the school will discipline any breach of the E-Safety Policy or of the school's acceptable use of ICT agreement for pupils in line with the school's Behaviour Policy.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, and will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g., by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

• School newsletter.
• Social media.
• 'Advice for Parents' CEOP section of the school website.
• 'Wellbeing and Safeguarding Support' section of the school website.
• Parents' evenings.

Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A digital record is kept of users who have been granted internet access.

All members of the school community use the school's internet network, as it has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The LET Education Trust ensures the school's ICT network has appropriate filters and monitoring systems in place. The Trust ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The school uses the Lightspeed, Sophos and Impero filtering and monitoring services, which is proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system are directed to the IT support. Reports of what is being blocked and who has requested it are collated and actioned by the LET Education Trust. Reports of inappropriate websites or materials are made to an ICT Technician immediately, who then investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the 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 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 DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. The firewall is provided by Schools Broadband and is set to restrict access to the school network from the outside. Firewalls are switched on at all times. Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the ICT Technician.

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

Emails

Access to and the use of emails is managed in line with the Data Protection Policy.
Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement.
Personal email accounts are not permitted to be used on the school site. 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 Technician. 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.

The Computing curriculum and PSHE Education curriculum cover security issues, including the following:

- How to determine whether an email address is legitimate.
- The types of address a phishing email could use.
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email.

Any cyber-attacks initiated through emails are managed in line with the Data and E-security Breach Prevention and Management Plan.

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 can use personal social media during break and lunchtimes; however, staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Handbook contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff receive annual 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. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g., they are friends with a parent at the school, they will disclose this to the DSL/Headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

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

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g., Anti-Bullying Policy, Staff Code of Conduct and Behaviour for learning procedure.

Use on behalf of the school

The use of social media on behalf of the school is conducted on the school's official social media channels and are only used for official educational or engagement purposes. Staff members must be authorised by the Headteacher to access 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 school website

The Headteacher is responsible for the overall content of the school website – 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 permissions have been granted.

Use of devices - School-owned devices

Staff members may be issued with the following devices to assist with their work:

• Laptop/desktop computer

• Tablet

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g., laptops to use during lessons.

School-owned devices are used in accordance with the Staff Handbook. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected.

All school-owned computers are set to update software automatically. The ICT Technician will force an update as and when required, such as loading software as part of the general upkeep. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT Technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

Personal devices

Personal devices are used in accordance with the Staff ICT and Electronic Devices Policy.

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

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. 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 Whistleblowing 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 will inform the Police/LADO and action will be taken in line with the Safeguarding Policy.

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.

Remote learning

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 consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable –

alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, and allows for audio and visual material to be recorded or downloaded, where required.

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.

Appendices

Appendix A - Online harms and risks – curriculum coverage

How to navigate the internet and manage information

• Age restrictions

• Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.

Teaching includes the following:

o That age verification exists and why some online platforms ask users to verify their age

o Why age restrictions exist

o That content that requires age verification can be damaging to under-age consumers

o What the age of digital consent is (13 for most platforms) and why it is important

• How content can be used and shared

Knowing what happens to information, comments or images that are put online. Teaching includes the following:

o What a digital footprint is, how it develops and how it can affect pupils' futures

o How cookies work

o How content can be shared, tagged and traced

o How difficult it is to remove something once it has been shared online

o What is illegal online, e.g., youth-produced sexual imagery (sexting)

• Disinformation, Misinformation and hoaxes

Some information shared online is accidentally or intentionally wrong, misleading or exaggerated.
Teaching includes the following:
o Disinformation and why individuals or groups choose to share false information in order to deliberately deceive
o Misinformation and being aware that false and misleading information can be shared inadvertently
o Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons
o That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online
o How to measure and check authenticity online
o The potential consequences of sharing information that may not be true

Fake websites and scam emails

Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain.
Teaching includes the following:
o How to recognise fake URLs and websites
o What secure markings on websites are and how to assess the sources of emails
o The risks of entering information to a website which is not secure
o What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email
o Who pupils should go to for support

Online fraud

Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following:
o What identity fraud, scams and phishing are
o That children are sometimes targeted to access adults' data
o What 'good' companies will and will not do when it comes to personal details

Password phishing

Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following:
o Why passwords are important, how to keep them safe and that others might try to get people to reveal them

o How to recognise phishing scam

o The importance of online security to protect against viruses that are designed to gain access to password information

o What to do when a password is compromised or thought to be compromised

Personal data

Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following:

o How cookies work

o How data is farmed from sources which look neutral

o How and why personal data is shared by online companies

o How pupils can protect themselves and that acting quickly is essential when something happens

o The rights children have with regards to their data

o How to limit the data companies can gather

Persuasive design

Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following:

o That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible

o How notifications are used to pull users back online

Privacy settings

Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following:

o How to find information about privacy settings on various devices and platforms

o That privacy settings have limitations

Targeting of online content

Much of the information seen online is a result of some form of targeting. Teaching includes the following:

o How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts

o How the targeting is done

o The concept of clickbait and how companies can use it to draw people to their sites and services

How to stay safe online

• Online abuse

Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following:

o The types of online abuse, including sexual harassment, bullying, trolling and intimidation

o How to respond to online abuse and how to access support

o How to respond when the abuse is anonymous

o The potential implications of online abuse

o What acceptable and unacceptable online behaviours look like

Challenges

Online challenges acquire mass followings and encourage others to take part in what they suggest.

Teaching includes the following:

o What constitutes a 'dare' and how these 'challenges' may be presented online

o Understanding that, while some challenges will be fun and harmless, others may be dangerous and even illegal

o How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why

o That it is okay to say no and to not take part in a dare or challenge

o How and where to go for help

o The importance of telling an adult about dares or challenges which include threats or secrecy, such as 'chain letter' style challenges

Content which incites violence

Knowing that violence can be incited online and escalate very quickly into offline violence.

Teaching includes the following:

o That online content (sometimes gang related) can glamorise the possession of

o weapons and drugs

o That to intentionally encourage or assist in an offence is also a criminal offence

o How and where to get help if they are worried about involvement in violence

Fake profiles

Not everyone online is who they say they are. Teaching includes the following:

o That, in some cases, profiles may be people posing as someone they are not or may be 'bots'

o How to look out for fake profiles

Grooming

Knowing about the different types of grooming and motivations for it, e.g., radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following:

o Recognising what makes a healthy relationship and understanding what to do if a relationship changes and no longer feels healthy

o Boundaries in friendships with peers, in families, and with others

o Key indicators of grooming behaviour

o The importance of telling a trusted adult if anything they see, hear or are asked to do makes them feel uncomfortable

o How and where to report these issues, both in school and to the police

At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.

Livestreaming

Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following:

o What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content

o The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely

o That online behaviours should mirror offline behaviours and that this should be considered when making a livestream

o That pupils should not feel pressured to do something online that they would not do offline

o Why people sometimes do and say things online that they would never consider appropriate offline

o The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next

Unsafe communication

Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following:

o That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with

o How to identify indicators of risk and unsafe communications

o The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before

o What online consent is and how to develop strategies to confidently say no to both friends and strangers online

Wellbeing

• Impact on confidence (including body confidence)

Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following:

o The issue of using image filters and digital enhancement

o The role of social media influencers, including that they are paid to influence the behaviour of their followers

o The issue of photo manipulation, including why people do it and how to look out for it

Impact on quality of life, physical and mental health and relationships

Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following:

o How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)

o How to consider quality vs. quantity of online activity

o The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out That time spent online gives users less time to do other activities, which can lead some users to become physically inactive

o The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues

o That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support

o Where to get help

Online vs. offline behaviours

People can often behave differently online to how they would act face to face. Teaching includes the following:

o How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives

o How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face

• Suicide, self-harm and eating disorders

Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.

Potential issues arising

AI (Government urging a policy)