



Digital Resilience Strategy

Approved by: FGB

Date: September 2021

Last reviewed on: June 2026

Next review due by: June 2027

1.0 Strategy Overview

1.1 Strategy Statement

Newport Primary School recognises that technology is an integral part of children's lives and that safeguarding children in the digital world is an essential part of safeguarding children in the real world.

Digital Resilience is a whole-school responsibility. We are committed to creating a culture where pupils, staff, governors and parents can use technology safely, responsibly and positively. We believe that children should be equipped with the knowledge, skills and confidence to access the benefits of technology whilst understanding and managing the risks that can arise from being online.

The school's approach to Digital Resilience goes beyond simply preventing harm. We aim to develop digitally resilient learners who can recognise risk, make informed choices, seek help when needed and recover from adverse online experiences. Through effective teaching, strong safeguarding procedures and partnership working with parents and carers, we seek to promote positive digital citizenship and prepare pupils for life in an increasingly connected world.

This strategy sets out how Newport Primary School promotes safe and responsible use of technology, supports pupils to navigate the online world confidently and responds to online safety concerns. It outlines expectations for all members of the school community and establishes clear procedures for preventing, identifying and responding to digital safeguarding issues.

The strategy has been informed by:

- Department for Education, Keeping Children Safe in Education (updated annually)
- Working Together to Safeguard Children
- Education Act 2011
- Counter-Terrorism and Security Act 2015
- Prevent Duty Guidance
- Online Safety Act 2023
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Department for Education, Teaching Online Safety in Schools (2023)
- DfE Filtering and Monitoring Standards for Schools and Colleges
- UK Council for Internet Safety (UKCIS), Education for a Connected World Framework
- UK Council for Internet Safety (UKCIS), Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People (updated 2024)
- Relationships Education, Relationships and Sex Education (RSE) and Health Education Statutory Guidance
- Computer Misuse Act 1990

Our approach is underpinned by the belief that children should be empowered to use technology as a force for learning, creativity, communication and personal development, while being equipped to recognise, manage and report any risks they may encounter online. This includes emerging risks associated with social media, online gaming, misinformation, cyberbullying, online exploitation, artificial intelligence and other developing technologies.

By working together as a school community, we aim to ensure that all pupils leave Newport Primary School as safe, responsible and resilient digital citizens who are prepared for the opportunities and challenges of modern life.

This strategy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Artificial Intelligence (AI) Policy
- Data Protection Policy
- Acceptable Use Agreements

This strategy is published on the school's website and is available to staff, governors, parents and carers. Digital resilience and online safety are embedded throughout the curriculum and wider safeguarding culture of the school.

1.2 Digital Resilience and Newport Primary School

Technology plays an increasingly important role in the lives of children and young people. Newport Primary School recognises the importance of equipping pupils with the knowledge, skills and confidence to use digital technologies safely, responsibly and positively throughout their lives.

Digital resilience is the ability to understand, recognise and respond appropriately to risks encountered when using technology and online services. It enables children to make informed decisions, seek support when required, learn from their experiences and recover from negative online experiences.

We aim to develop digitally resilient pupils who are able to:

- Recognise when they may be at risk online.
- Make safe and informed choices when using technology.
- Know where to go and who to speak to if they need help or support.
- Think critically about online content and information.
- Learn from their own experiences and the experiences of others.
- Recover positively when things go wrong online.
- Use technology safely, respectfully and responsibly.

At Newport Primary School, we promote a culture of positive digital citizenship. We want our pupils to understand that technology can be a powerful force for learning, creativity, communication and personal development. Through our curriculum, safeguarding procedures and wider school culture, we support pupils to become increasingly independent, responsible and confident users of technology who are prepared for the opportunities and challenges of an ever-evolving digital world.

2. Roles and Responsibilities

Governing Body

The Governing Body is responsible for:

- Ensuring this strategy is implemented and reviewed annually.
- Monitoring the effectiveness of the school's digital safeguarding arrangements.
- Receiving regular updates regarding online safety, filtering and monitoring, digital safeguarding incidents and emerging risks.
- Ensuring appropriate resources, policies and staff training are in place.
- Providing strategic oversight of digital safeguarding within the school.

Headteacher

The Headteacher is responsible for:

- Ensuring the effective implementation of this strategy.
- Promoting a positive culture of digital safeguarding and resilience.
- Ensuring staff receive appropriate training and support.
- Working with the DSL and Governors to monitor and review digital safeguarding arrangements.
- Ensuring concerns are acted upon appropriately and in a timely manner.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (and Deputy DSLs) are responsible for:

- Acting as the lead professionals for all digital safeguarding concerns.
- Assessing and responding to online safety incidents and concerns.
- Recording and monitoring incidents using CPOMS.
- Supporting staff, pupils and families with digital safeguarding matters.
- Keeping up to date with current guidance, legislation and emerging online risks.
- Working with external agencies where required.
- Overseeing the effectiveness of filtering and monitoring arrangements.

Computing Lead

The Computing Lead is responsible for:

- Supporting the delivery of the computing and online safety curriculum.
- Promoting digital resilience across the school.
- Supporting staff with developments in technology and online safety education.
- Working alongside the DSL to identify emerging trends and risks.
- Supporting the review and development of this strategy.

All Staff

All staff are responsible for:

- Safeguarding children online as part of their wider safeguarding responsibilities.
- Modelling safe, responsible and professional use of technology.
- Following school policies and acceptable use agreements.
- Reporting concerns promptly to the DSL.
- Remaining vigilant to online safety concerns and emerging risks.

- Participating in regular safeguarding and online safety training.

Pupils

Pupils are expected to:

- Use technology safely, respectfully and responsibly.
- Follow school acceptable use expectations.
- Report concerns or worries about online content, contact or conduct to a trusted adult.
- Demonstrate positive digital citizenship.

Parents and Carers

Parents and carers are encouraged to:

- Support the school's online safety messages.
- Promote safe use of technology at home.
- Report concerns to the school where appropriate.
- Work in partnership with the school to support children's digital resilience.

2.0 Technology and Learning at Newport Primary School

2.1 The Use of Technology in School

Technology is an integral part of teaching, learning, communication and safeguarding within Newport Primary School. We recognise that digital technologies provide valuable opportunities to enhance learning, improve outcomes for pupils and prepare children for life in an increasingly digital society.

Technology is used to:

- Support high-quality teaching and learning across the curriculum.
- Develop pupils' digital literacy, computing and problem-solving skills.
- Promote creativity, collaboration and communication.
- Enable access to educational resources and learning platforms.
- Support inclusion and accessibility for all learners.
- Facilitate effective communication between school, parents and external agencies.
- Improve the efficiency of school administration and management systems.
-

We want all pupils to develop the knowledge, skills and confidence to use technology safely, respectfully and responsibly. Through our curriculum and wider safeguarding provision, pupils are supported to become capable, resilient and responsible digital citizens who are prepared for the opportunities and challenges of modern life.

2.2 Benefits of Technology and the Internet

The appropriate use of technology and the internet offers significant educational benefits for pupils, staff and the wider school community, including:

- Access to a wide range of educational resources and learning opportunities.
- Access to museums, galleries, libraries and cultural experiences from around the world.
- Opportunities for research, investigation and independent learning.

- Access to remote and blended learning platforms when required.
- Development of communication, collaboration and creativity skills.
- Support for pupils with additional needs through accessible technologies.
- Opportunities to engage with online safety and digital citizenship education.
- Professional development opportunities for staff.
- Communication and collaboration with educational partners, support services and external organisations.
- Secure management of school and pupil information.

While technology provides many benefits, Newport Primary School also recognises the need to educate pupils about potential online risks. Through an embedded programme of digital resilience, online safety and media literacy education, pupils learn how to use technology safely, critically and responsibly.

2.3 Computing and Digital Resilience Curriculum

The school delivers a broad and balanced computing curriculum in line with the National Curriculum requirements.

Through computing, RSHE, assemblies and wider safeguarding education, pupils are taught to:

- use technology safely, respectfully and responsibly;
- protect their personal information online;
- understand online risks and how to seek support;
- evaluate online information critically;
- communicate appropriately online;
- recognise and report concerns relating to content, contact, conduct and commerce;
- understand the opportunities and risks associated with emerging technologies, including artificial intelligence.

Pupils are also taught age-appropriate knowledge and skills relating to:

- online relationships;
- cyberbullying;
- media literacy;
- misinformation and disinformation;
- privacy and security;
- online reputation;
- digital citizenship.

Teaching is progressive and builds upon pupils' prior knowledge and experiences as they move through the school.

2.4 Digital Safeguarding, Media Literacy and Emerging Technologies

Digital safeguarding and online safety are embedded throughout the curriculum and wider life of Newport Primary School. While key knowledge and skills are taught through the Computing curriculum, pupils also develop their understanding of online safety, digital resilience and

responsible technology use through RSHE, assemblies, safeguarding activities, external visitors and other curriculum areas.

The school uses a range of age-appropriate educational resources and programmes to support the teaching of digital resilience and online safety. These may include resources from organisations such as **Be Internet Legends, CEOP Education, Childnet, Internet Matters and the UK Safer Internet Centre.**

Through an age-appropriate and progressive curriculum, pupils are supported to become safe, confident and responsible users of technology. Teaching includes:

- Online relationships and respectful communication.
- Cyberbullying and online harm.
- Privacy, consent and personal information.
- Online reputation and digital footprints.
- Media literacy and critical thinking.
- Misinformation, disinformation and fake news.
- Body image and the influence of social media.
- Online scams, persuasion and commercial risks.
- Reporting concerns and accessing support.
- Emerging technologies, including Artificial Intelligence (AI).

2.4.1 Evaluating Online Information

Pupils are taught that not all information found online is accurate, reliable or trustworthy. As part of their learning, pupils are encouraged to think critically about the content they encounter and to question the reliability of online sources.

Teaching may include:

- Recognising that online content may be inaccurate, misleading or deliberately deceptive.
- Understanding that websites, social media content and AI-generated content may contain errors or bias.
- Evaluating the credibility and reliability of sources.
- Understanding how search engines and online platforms present information.
- Recognising misinformation, disinformation and fake news.
- Respecting copyright and intellectual property.
- Understanding the importance of citing sources where appropriate.
- Knowing how and when to seek help if they encounter content that concerns, upsets or confuses them.

2.4.2 Emerging Technologies

The school recognises that technology continues to evolve rapidly. New technologies and digital tools will be considered carefully before being introduced into school.

Where appropriate, the school will assess:

- Educational benefits.
- Safeguarding implications.

- Privacy and data protection considerations.
- Suitability for the age and needs of pupils.
- Potential risks associated with emerging technologies.

Appropriate risk assessments will be undertaken where required to ensure that new technologies are used safely, responsibly and in accordance with the school's safeguarding expectations.

2.4.3 Online Safety and SEND

Newport Primary School recognises that some pupils with Special Educational Needs and Disabilities (SEND) may be more vulnerable to online risks and may require additional support to develop digital resilience.

The school will ensure that online safety education is accessible to all pupils and, where necessary, teaching, resources and interventions will be adapted to meet individual needs. Staff will consider pupils' age, stage of development, communication needs and understanding when delivering online safety education and responding to digital safeguarding concerns.

Where appropriate, additional support will be provided to help pupils:

- Understand online risks.
- Recognise unsafe situations.
- Develop safe online behaviours.
- Report concerns and seek help.
- Build confidence and resilience when using technology.
-

This approach supports the school's commitment to ensuring that all pupils can participate safely and successfully in an increasingly digital world.

2.4.4 Acceptable Use

Technology is an important part of teaching, learning and communication at Newport Primary School. All members of the school community are expected to use technology safely, responsibly and in accordance with school expectations.

The school maintains separate Acceptable Use Agreements for:

- Staff
- Pupils

These agreements outline the expectations for the safe and appropriate use of:

- School devices
- Internet access
- Email systems
- Learning platforms
- Digital communication tools
- Emerging technologies
-

All users are expected to:

- Use technology safely, respectfully and responsibly.
- Protect personal information and the privacy of others.
- Follow safeguarding, behaviour and data protection requirements.
- Report concerns or inappropriate content promptly.
- Respect the rights, wellbeing and dignity of others when communicating online.

The school reserves the right to monitor the use of its devices, systems and network in order to safeguard pupils, protect users and ensure compliance with school policies and statutory requirements.

Any misuse of school technology may result in action being taken in accordance with the school's Behaviour Policy, Staff Code of Conduct, Safeguarding and Child Protection Policy or other relevant procedures.

2.5 Reporting, Consultation and Review

Newport Primary School recognises that digital technologies and online risks change rapidly. The school will work collaboratively with staff, pupils, parents and governors to ensure that this strategy remains effective, relevant and responsive to emerging issues.

Staff will receive regular safeguarding and online safety training appropriate to their role and responsibilities. Opportunities will be provided for staff to discuss emerging risks, share concerns and contribute to the ongoing development of the school's digital resilience arrangements. Pupil voice, parental feedback and staff consultation may be used to inform the review and development of this strategy and related policies.

Concerns relating to the misuse of technology, online safety, digital safeguarding or inappropriate online behaviour should be reported to the Designated Safeguarding Lead (DSL) or Headteacher as appropriate. Any safeguarding concerns will be managed in accordance with the school's Child Protection and Safeguarding Policy. Complaints relating to the use of technology or online services will be managed in accordance with the school's Complaints Policy.

3.0 Management of School Technology Systems

3.1 Technology Management and Security

Newport Primary School recognises that secure and reliable technology systems are essential to support teaching, learning, administration and safeguarding. The school works with its designated IT support provider to ensure that technology systems are maintained appropriately and remain secure, effective and suitable for educational use.

The school will ensure that reasonable measures are in place to:

- Maintain the security and integrity of school systems and devices.
- Protect personal and sensitive information.

- Support effective filtering and monitoring arrangements.
- Manage user access and permissions appropriately.
- Protect devices and systems from malicious software and cyber threats.
- Maintain appropriate backup and recovery arrangements.
- Ensure software and systems are regularly maintained and updated.
- Support staff in using technology safely and responsibly.
- Respond appropriately to security incidents and system vulnerabilities.

All members of the school community have a responsibility to help maintain the security of school systems by following school policies, using technology responsibly and reporting any concerns promptly.

The school recognises that cyber security forms an important part of safeguarding and operational resilience. Cyber incidents can impact the confidentiality, integrity and availability of safeguarding information, pupil records and school systems.

Detailed operational arrangements relating to cyber security, system management, incident response, password management, access controls and technical security measures are contained within the school's Cyber Security Policy.

3.2 Information Security and Data Protection

Newport Primary School is committed to ensuring that personal information is collected, stored, processed and shared securely and in accordance with current data protection legislation.

The school recognises that the secure handling of information is an important part of safeguarding and protecting the welfare of pupils, staff and the wider school community.

The school will:

- Comply with the requirements of the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).
- Ensure that access to personal and sensitive information is restricted to authorised individuals who require it for their role.
- Use approved and secure systems for the storage, processing and transfer of information.
- Take appropriate steps to protect information from loss, unauthorised access, misuse or disclosure.
- Ensure that staff receive appropriate guidance and training regarding information security and data protection.
- Report and manage any data breaches or information security incidents in accordance with school procedures.

All staff are responsible for maintaining the confidentiality and security of information they access as part of their role. Staff must ensure that personal information is handled appropriately, shared only when necessary and stored securely in accordance with school procedures.

Where information is transferred electronically, approved and secure methods of communication must be used. Sensitive or confidential information must not be shared through personal accounts, unsecured systems or unauthorised applications.

Further information relating to the collection, storage, sharing and protection of personal data can be found within the school's Data Protection Policy, Records Management Procedures and Cyber Security Policy.

3.3 Filtering and Monitoring

Newport Primary School recognises that effective filtering and monitoring systems form an essential part of safeguarding pupils and staff when using technology. The school implements appropriate filtering and monitoring arrangements to reduce the risk of users accessing unlawful, inappropriate, harmful or age-inappropriate content, whilst also supporting the identification of safeguarding concerns. Filtering and monitoring systems are designed to support, but not replace, effective supervision, staff vigilance and online safety education.

The school has designated a member of the Senior Leadership Team with responsibility for filtering and monitoring. This individual will work with the Designated Safeguarding Lead and in partnership with the school's IT support provider to oversee filtering and monitoring arrangements and to undertake the required annual review of effectiveness.

Filtering and monitoring arrangements are intended to:

- Protect pupils and staff from accessing harmful, inappropriate or illegal content.
- Support compliance with safeguarding responsibilities.
- Help identify behaviour that may indicate a safeguarding concern.
- Support the prevention of online bullying, exploitation, radicalisation and other online harms.
- Assist the school in responding appropriately to safeguarding concerns.
- Support the safe use of emerging technologies, including AI-enabled services and online platforms.

3.3.1 Roles and Responsibilities

The Governing Body, Headteacher, Designated Safeguarding Lead (DSL) and IT support provider share responsibility for ensuring that filtering and monitoring arrangements are effective and appropriate.

The DSL will:

- Oversee safeguarding concerns identified through filtering and monitoring systems.
- Work with school leaders and IT support providers to review risks and incidents.
- Ensure appropriate action is taken where concerns are identified.
- Monitor trends and emerging safeguarding risks.

All staff are responsible for reporting any concerns regarding the effectiveness of filtering and monitoring systems to the DSL or Headteacher.

3.3.2 Review of Filtering and Monitoring

The school will review its filtering and monitoring arrangements annually and whenever significant changes occur to technology systems or safeguarding requirements. The review will take account of:

- The DfE Filtering and Monitoring Standards.
- Emerging safeguarding risks.
- New technologies and online platforms.
- Artificial intelligence and AI-generated content.
- Feedback from staff, pupils and governors.
- The effectiveness of current filtering and monitoring measures.

3.3.3 Reporting Concerns

If staff or pupils become aware of inappropriate content, safeguarding concerns or weaknesses in filtering arrangements, these must be reported immediately to the DSL.

Where a concern indicates a potential safeguarding risk, the matter will be recorded and managed in accordance with the school's Child Protection and Safeguarding Policy. Where unlawful content is identified, the school will follow appropriate reporting procedures and seek support from relevant agencies where required.

The school recognises that no filtering or monitoring system can completely eliminate risk. Therefore, filtering and monitoring are supported by effective supervision, staff training, age-appropriate online safety education and a culture in which pupils feel able to raise concerns and seek help when needed.

3.4 Safe Internet Access and Online Activity

Newport Primary School recognises the educational value of the internet and the opportunities it provides for learning, communication, creativity and collaboration. Access to online resources supports the delivery of the curriculum and helps prepare pupils for life in an increasingly digital world.

The school is committed to ensuring that internet access is provided in a safe, secure and age-appropriate manner. Access to online content is supported by filtering and monitoring systems, staff supervision, online safety education and clear expectations regarding acceptable use. These measures work together to reduce risk whilst allowing pupils to benefit from the opportunities that technology provides.

Pupils will be taught how to use the internet safely, respectfully and responsibly. This includes learning how to:

- Protect personal information and privacy.
- Communicate safely online.
- Evaluate the reliability and accuracy of online information.

- Recognise misinformation, disinformation and fake content.
- Understand the risks associated with social media, online gaming and online communication.
- Recognise and report inappropriate, harmful or concerning content.
- Seek help from a trusted adult when worried about something they have seen, heard or experienced online.
- Understand the opportunities and risks associated with emerging technologies, including artificial intelligence.

Pupils will be reminded that their use of school technology and internet access may be monitored for safeguarding purposes and that they must use school systems in accordance with the school's Acceptable Use Agreements.

Staff are responsible for:

- Providing appropriate supervision when pupils are using technology.
- Promoting safe and responsible online behaviours.
- Following the school's safeguarding procedures where concerns arise.
- Reporting inappropriate content, online safety concerns or potential weaknesses in filtering and monitoring arrangements to the Designated Safeguarding Lead (DSL).

If inappropriate or harmful online content is identified, appropriate action will be taken in accordance with the school's Child Protection and Safeguarding Policy. Where necessary, content may be reported to relevant agencies, including the Internet Watch Foundation (IWF), CEOP or the police.

While the school takes reasonable precautions to promote safe internet use, no filtering or monitoring system can eliminate all risk. For this reason, educating pupils to recognise, manage and respond appropriately to online risks remains a fundamental part of the school's approach to digital resilience and safeguarding.

3.5 Preventing Radicalisation and Extremism

Newport Primary School recognises that the internet, social media and online communication platforms can be used to promote extremist views, harmful ideologies, misinformation and content intended to influence or radicalise vulnerable individuals. The school acknowledges its responsibilities under the Prevent Duty and is committed to safeguarding pupils from all forms of extremism and radicalisation.

The school takes a proactive approach to reducing the risk of pupils being exposed to extremist or harmful online content through:

- Effective filtering and monitoring arrangements.
- Appropriate staff supervision.
- Online safety and digital resilience education.
- Promotion of critical thinking and media literacy skills.
- Teaching pupils how to recognise misinformation, disinformation and online manipulation.

- Encouraging pupils to speak to a trusted adult if they encounter content that concerns them.

Pupils are taught, in an age-appropriate manner, to:

- Question the accuracy and reliability of online information.
- Recognise attempts to influence, manipulate or exploit individuals online.
- Respect different viewpoints whilst challenging discrimination, prejudice and harmful behaviours.
- Report concerns about online content, communication or behaviour.

The school's filtering and monitoring systems are designed to help identify access to extremist, terrorist or other harmful content. Concerns identified through these systems will be reviewed by the Designated Safeguarding Lead (DSL) and managed in accordance with the school's safeguarding procedures.

Where concerns are identified that a pupil may be vulnerable to radicalisation or extremism, appropriate action will be taken in accordance with the school's Child Protection and Safeguarding Policy, Prevent Duty responsibilities and local safeguarding procedures.

3.6 Website and Published Content

Newport Primary School recognises that its website and digital communication platforms play an important role in communicating with pupils, parents, carers and the wider community. Digital publications should reflect the school's values, celebrate achievement and provide accurate and accessible information whilst maintaining the safety and privacy of pupils and staff.

The school will take reasonable steps to ensure that all published content:

- Reflects the values and ethos of the school.
- Is accurate, appropriate and regularly reviewed.
- Complies with safeguarding, data protection and copyright requirements.
- Protects the privacy and welfare of pupils and staff.
- Promotes a positive image of the school and its community.

The Headteacher and designated staff members are responsible for overseeing published content and ensuring that it remains appropriate and compliant with relevant legislation and school policies.

3.6.1 Photographs and Video Content

Photographs and videos can provide valuable opportunities to celebrate achievement and share learning experiences. However, the school recognises the importance of safeguarding pupils when publishing images.

The school will:

- Obtain and maintain appropriate parental consent for the use of pupil images.

- Use photographs and videos in accordance with the school's Data Protection Policy and media consent procedures.
- Carefully consider the suitability of images prior to publication.
- Avoid publishing information that could place pupils or staff at risk.
- Ensure that images are used respectfully and appropriately.
-

As a general principle:

- Full names of pupils will not be published alongside photographs.
- Personal contact details for pupils or staff will never be published.
- School contact details will be used for all official communications.
- Images will be selected carefully to maintain pupil dignity and privacy.

3.6.2 Social Media and Digital Communication

Where the school uses social media or other digital communication platforms, these will be managed in accordance with the school's Social Media expectations, safeguarding procedures and professional standards.

Digital platforms may be used to:

- Share school news and events.
- Celebrate pupil achievements.
- Communicate key information to families.
- Promote school initiatives and activities.

Comments, contributions and interactions on school-managed digital platforms should be respectful, appropriate and consistent with the school's values.

Any concerns relating to published content, images or online communications should be reported to the Headteacher or Designated Safeguarding Lead and will be managed in accordance with relevant school policies.

3.7 Email and Digital Communications

Email and digital communication systems are important tools for teaching, learning, administration and communication. Newport Primary School expects all users to communicate responsibly, professionally and in accordance with the school's safeguarding, data protection and acceptable use expectations.

The school provides approved communication systems for educational and business purposes. All users should recognise that the use of school communication systems is not private and may be monitored where necessary to support safeguarding, security, operational or legal requirements.

3.7.1 Staff Use

Staff are expected to:

- Use school-approved communication systems for all professional communications.
- Maintain appropriate professional boundaries when communicating with pupils, parents and carers.
- Ensure communications are professional, respectful and appropriate at all times.
- Consider safeguarding, confidentiality and data protection requirements before sharing information.
- Report any inappropriate, suspicious, threatening or concerning communications to the Headteacher or Designated Safeguarding Lead (DSL).
- Follow the requirements of the Staff Code of Conduct, Data Protection Policy and Acceptable Use Agreement.

Staff must not use personal email accounts, social media platforms or personal messaging applications to communicate with pupils unless specifically authorised by the school and supported by appropriate safeguarding arrangements.

3.7.2 Pupil Use

Where pupils are provided with access to email or digital communication tools, these will be managed in an age-appropriate manner and supported by appropriate safeguarding, filtering and monitoring arrangements.

Pupils will be taught to:

- Communicate respectfully and responsibly online.
- Protect personal information and privacy.
- Report any communication that causes concern.
- Recognise inappropriate, suspicious or unsafe messages.
- Understand the risks associated with online communication.
- Identify common online risks such as phishing, scams and impersonation.

Pupils must not use school communication systems to send offensive, threatening, inappropriate or harmful content.

3.7.3 Communication Security

The school will take reasonable steps to ensure that digital communication systems are secure and appropriate for educational use. This may include:

- Filtering and monitoring arrangements.
- Security and anti-malware protections.

- User authentication and access controls.
- Secure management of staff and pupil accounts.

Any misuse of email or digital communication systems will be managed in accordance with the Behaviour Policy, Staff Code of Conduct, Child Protection and Safeguarding Policy, Acceptable Use Agreements and other relevant school procedures.

3.8 School Devices and Off-Site Use

Newport Primary School recognises that technology may be used beyond the school site to support learning, communication and other educational activities. The same expectations for safe, responsible and appropriate use of technology apply whether devices are used in school or elsewhere.

School-owned devices are provided primarily to support teaching, learning and educational activities. Pupils and staff are expected to use these devices in accordance with the school's Acceptable Use Agreements, safeguarding expectations and relevant school policies.

3.8.1 School-Owned Devices

School-owned devices remain subject to the school's filtering and monitoring arrangements when used away from the school site. The school may investigate alerts or concerns identified through these systems and take appropriate safeguarding action where required.

Misuse of school devices may result in restricted access to equipment, withdrawal of usage privileges or other appropriate action in line with the school's Behaviour Policy, Staff Code of Conduct, Child Protection and Safeguarding Policy or other relevant procedures.

3.8.2 Expectations for Use

Users of school devices are expected to:

- Use devices safely, responsibly and for appropriate educational purposes.
- Protect passwords, accounts and personal information.
- Report any loss, damage, theft or security concern promptly.
- Follow school safeguarding, data protection and acceptable use expectations.
- Respect the privacy, rights and wellbeing of others when using technology.

Users must not:

- Attempt to bypass the school's filtering or monitoring systems.
- Access inappropriate, harmful or illegal content.
- Install unauthorised software or applications.
- Use devices in ways that could compromise the security of school systems or data.

- Engage in behaviour that may place themselves or others at risk.

3.8.3 Home Use and Parental Support

Where pupils use school devices at home, parents and carers are encouraged to support safe and responsible use of technology and reinforce the school's digital resilience messages.

The school recognises the importance of partnership working with families and will continue to promote safe, balanced and age-appropriate use of technology both in and out of school.

3.9 Reporting Concerns

Newport Primary School recognises that online safety and digital safeguarding concerns may arise through the use of technology, online services, digital communications, social media platforms and emerging technologies. All members of the school community have a responsibility to report concerns promptly so that appropriate support and safeguarding action can be taken.

Staff should remain vigilant to signs that a pupil may be experiencing online harm or be at risk through their use of technology. This may include concerns relating to:

- Online bullying, harassment or abuse.
- Inappropriate, harmful or illegal online content.
- Exploitation, grooming or coercion.
- Radicalisation or extremist content.
- The sharing of nude or semi-nude images.
- Misuse of artificial intelligence (AI) technologies.
- Misinformation, disinformation or online manipulation.
- Any behaviour that may place a child at risk of harm.

Concerns may be identified through:

- Staff observations.
- Pupil disclosures.
- Filtering and monitoring systems.
- Parents and carers.
- External agencies.
- Online reports or referrals.
- School-owned devices used on or off-site.

Any safeguarding concern must be reported to the Designated Safeguarding Lead (DSL) without delay.

Online safety concerns will be recorded and managed in accordance with the school's Child Protection and Safeguarding Policy. Records will be maintained using the school's safeguarding recording system and appropriate action taken in response to the level of risk identified.

Where appropriate, concerns may be referred to external agencies including Children's Social Care, the Police, CEOP, the Internet Watch Foundation (IWF) or other relevant safeguarding partners.

The school promotes a culture in which pupils feel confident to report concerns, ask for help and discuss their online experiences. Pupils are reminded regularly that speaking to a trusted adult is one of the most effective ways to stay safe online.

Section 4 – Social Media and Online Communication

4.1 Social Media and Online Platforms

Newport Primary School recognises that social media, online communication platforms and content-sharing services form an increasingly significant part of children's lives. While many of these technologies provide opportunities for communication, learning, creativity and collaboration, they can also present safeguarding risks.

The term *social media* includes social networking sites, messaging services, online forums, content-sharing platforms, livestreaming services, gaming communication platforms and emerging digital communication technologies.

The school recognises that children may encounter social media and similar technologies both directly and indirectly, regardless of age restrictions applied by individual platforms. Therefore, online safety education focuses on developing pupils' knowledge, critical thinking and digital resilience so that they can recognise and respond appropriately to online risks.

4.2 Teaching Safe Use of Social Media

The school is committed to ensuring that pupils understand how to use online platforms safely, responsibly and respectfully.

Teaching about social media is integrated throughout the Computing curriculum, RHE, assemblies, safeguarding education and wider curriculum opportunities. Age-appropriate resources such as Be Internet Legends, CEOP Education and other recognised online safety programmes may be used to support learning.

Pupils will be taught about:

- Online relationships and respectful communication.
- Privacy, consent and the protection of personal information.
- Digital footprints and online reputation.
- Cyberbullying, online abuse and harmful behaviours.
- Misinformation, disinformation and fake news.
- Influencer culture and online persuasion.

- Body image and wellbeing online.
- Livestreaming and online gaming risks.
- Artificial Intelligence (AI), deepfakes and AI-generated content.
- Anonymous messaging and online communication.
- Commercial risks such as scams, fraud and inappropriate advertising.
- How and when to seek help from a trusted adult.

Pupils will also be taught to understand the four key areas of online risk:

- **Content** – material encountered online.
- **Contact** – interaction with others online.
- **Conduct** – behaviour online.
- **Commerce** – commercial risks and exploitation.

The school promotes positive digital citizenship and seeks to develop pupils who can make informed decisions, recognise risks, act responsibly and seek support when needed.

4.3 Social Media Expectations for Pupils

Pupils are expected to:

- Treat others with kindness and respect online.
- Follow the school's Acceptable Use Agreement.
- Protect their personal information.
- Report concerns or worries to a trusted adult.
- Refrain from posting harmful, offensive or inappropriate content.
- Consider the impact of their online behaviour on themselves and others.

Pupils should understand that information shared online may remain accessible even after it has been deleted and that online actions can have real-world consequences.

4.4 Parents, Carers and Digital Resilience

Newport Primary School recognises the important role that parents and carers play in supporting children to navigate the online world safely.

The school aims to work in partnership with families by:

- Providing online safety information and guidance.
- Sharing updates about emerging online risks.
- Offering digital resilience and online safety workshops where appropriate.
- Signposting parents and carers to trusted online safety resources.
- Promoting positive digital habits and healthy technology use.
- Supporting parents in understanding learning platforms and educational technologies used by the school.

Parents and carers are encouraged to:

- Take an active interest in their child's online activities.
- Discuss online safety regularly.
- Use appropriate parental controls and privacy settings.
- Encourage children to report anything that worries or upsets them online.
- Work in partnership with the school when online safety concerns arise.

4.5 Staff Professional Conduct Online

The school recognises that staff may use social media and other online platforms in their personal lives. Staff are expected to maintain appropriate professional standards at all times and act in a manner that protects both themselves and the reputation of the school.

Staff must:

- Follow the Staff Code of Conduct and Acceptable Use Agreement.
- Maintain appropriate professional boundaries.
- Protect confidential information.
- Use professional judgement when publishing content online.
- Report concerns relating to online safety or professional conduct.

Staff must not:

- Accept friend or follow requests from current pupils through personal accounts.
- Initiate personal contact with pupils through social media or personal messaging platforms.
- Publish confidential information relating to the school, pupils, families or colleagues.
- Post material that could bring themselves or the school into disrepute.
- Use personal online accounts for school business.

Any concerns relating to staff conduct online will be managed in accordance with the Staff Code of Conduct and relevant school procedures.

4.6 Reporting Social Media Concerns

Anyone who becomes aware of inappropriate online behaviour, unsafe social media activity or safeguarding concerns should report them promptly to the Designated Safeguarding Lead (DSL).

Concerns may include:

- Cyberbullying.
- Online harassment.
- Harmful content.
- Inappropriate contact.
- Sharing of personal information.
- Online exploitation.
- Radicalisation.

- AI-generated abuse or manipulation.
- Any activity that may place a child at risk.

Concerns will be investigated and managed in accordance with the school's Child Protection and Safeguarding Policy.

4.7 Social Media, Extremism and Radicalisation

The school recognises that social media and online platforms may expose children and young people to extremist content, misinformation, conspiracy theories, manipulation and radicalisation.

Through the curriculum and wider safeguarding provision, pupils are taught to:

- Think critically about online information.
- Question the reliability of online sources.
- Recognise attempts to manipulate or influence opinions.
- Challenge harmful stereotypes and prejudice.
- Report content that concerns them.
-

Concerns relating to radicalisation, extremism or harmful online influence will be managed in accordance with the school's Child Protection and Safeguarding Policy, Prevent Duty responsibilities and local safeguarding procedures.

5.0 Mobile devices: Staff, pupils and parents

5.1 Staff

- Staff must not use mobile phones in classrooms at any time when pupils are present
- Staff are permitted to use their devices in staff rooms, meeting rooms or classrooms during break and lunchtime if no pupils are present
- Staff are not permitted to take photos or videos of students on personal devices, if photos or videos are being taken for curriculum or professional use then school devices (i.e. iPad, digital camera) should be used.
- Mobile devices should be switched to silent during school hours.

5.2 Pupils

Pupils are not permitted to bring mobile phones or personal internet-enabled devices into school unless specific permission has been granted by the Headteacher or Deputy Headteacher in exceptional circumstances.

If a pupil is found with a device they can be legally confiscated by the Head Teacher under section 94 of the Education and Inspection Act 2006.

6.0 Specific Digital Safeguarding issues

6.1 Staff Training

All staff receive regular safeguarding and online safety training appropriate to their role and responsibilities. Training is updated regularly to reflect changes in legislation, technology and emerging online risks.

Staff will be made aware of:

- The school's Digital Resilience Strategy.
- Their safeguarding responsibilities in relation to online safety.
- Current and emerging digital safeguarding risks.
- The school's filtering and monitoring arrangements.
- Procedures for reporting concerns.
- Child-on-child abuse in both online and offline contexts.
- Online exploitation, radicalisation, cyberbullying and the sharing of nude or semi-nude images.
- Risks associated with social media, gaming platforms, livestreaming, misinformation and artificial intelligence (AI).
-

Digital safeguarding updates will form part of ongoing safeguarding training, staff meetings and professional development activities.

6.2 Child-on-Child Abuse

Newport Primary School recognises that safeguarding issues can manifest themselves through child-on-child abuse, both online and offline. All concerns will be taken seriously and managed in accordance with the school's Child Protection and Safeguarding Policy.

Child-on-child abuse may include:

- Bullying, including cyberbullying.
- Sexual harassment, including online sexual harassment.
- Sharing of nude or semi-nude images.
- Upskirting.
- Harmful online communication.
- Manipulation or coercion through messaging platforms.
- Sharing, creating or distributing altered, manipulated or AI-generated images intended to cause harm, distress or humiliation.
- Harmful behaviour through social media, gaming platforms or group chats.

The school recognises the gendered nature of some forms of child-on-child abuse but acknowledges that all children can be affected and all concerns will be investigated appropriately.

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

Newport Primary School recognises that child sexual exploitation (CSE) and child criminal exploitation (CCE) can occur online as well as offline.

Online exploitation may involve:

- Grooming.
- Manipulation and coercion.
- Requests for personal information.
- The sharing of images or videos.
- Online friendships established for exploitative purposes.
- Encouragement to engage in illegal or harmful activity.
-

Indicators may include:

- Increased secrecy about online activity.
- Sudden changes in behaviour or emotional wellbeing.
- Unexplained gifts, rewards or online purchases.
- Excessive use of devices.
- Multiple online accounts.
- Contact with unknown individuals online.
- Withdrawal from normal activities.

Any concerns must be reported immediately to the Designated Safeguarding Lead (DSL) and managed in accordance with the school's Child Protection and Safeguarding Policy. Where a child is believed to be at immediate risk of harm, the Police and/or Children's Social Care will be contacted without delay.

6.4 Sharing Nudes and Semi-Nudes

The school recognises that incidents involving the creation or sharing of nude or semi-nude images can occur both online and offline. Any incident involving the sharing of nude or semi-nude images will be treated as a safeguarding concern and managed in accordance with current UK Council for Internet Safety (UKCIS) guidance and the school's Child Protection and Safeguarding Policy.

Staff should:

- Report incidents immediately to the DSL.
- Avoid viewing or forwarding images unless absolutely necessary.
- Follow safeguarding procedures carefully.
- Not investigate incidents independently.

Pupils will be taught about:

- Consent.
- Privacy.
- Online reputation.
- The potential consequences of sharing images.
- How to seek support if concerns arise.

6.5 Emerging Online Safeguarding Risks

6.5.1 Artificial Intelligence (AI), Deepfakes and Manipulated Content

Newport Primary School recognises that Artificial Intelligence (AI) technologies are increasingly accessible to children and young people and may present both opportunities and safeguarding risks. Pupils may encounter AI-generated content through search engines, chatbots, social media platforms, gaming environments and other online services.

As part of the school's digital resilience curriculum, pupils will be taught to:

- Think critically about online information and images.
- Understand that AI-generated content may not always be accurate or reliable.
- Recognise that images, videos and audio recordings may be altered or generated using AI.
- Understand the risks associated with deepfakes, misinformation and online manipulation.
- Use technology safely, responsibly and ethically.
- Seek support from a trusted adult if they encounter concerning online content.
-

Staff will remain vigilant to safeguarding concerns relating to AI-generated content, image manipulation, impersonation, cyberbullying and other emerging technologies.

Further guidance regarding the use, management and governance of Artificial Intelligence is contained within the school's Artificial Intelligence (AI) Policy.

6.5.2 Livestreaming and Live Content

The school recognises that livestreaming and live communication platforms are increasingly popular with children and young people. Whilst livestreaming can provide opportunities for creativity and communication, it also presents safeguarding risks.

These risks may include:

- Contact with unknown individuals.
- Online grooming and exploitation.
- Exposure to inappropriate content.
- Cyberbullying and harassment.
- Pressure to share personal information.
- Recording or redistribution of content without permission.
- Exposure to harmful challenges or trends.
- Financial exploitation through gifts, donations or paid interactions.

Pupils will be taught to:

- Protect their privacy.
- Avoid sharing identifying information.
- Use privacy settings appropriately.
- Report inappropriate behaviour or content.
- Seek support from a trusted adult when concerned.

6.5.3 Misinformation and Disinformation

The school recognises that children are increasingly exposed to misleading, inaccurate or deliberately deceptive online content.

Pupils will be taught to:

- Evaluate information critically.
- Verify information from multiple sources.
- Recognise fake news.
- Understand how online algorithms influence content.
- Identify unreliable or misleading sources.
- Consider the purpose and motivation behind online content.

6.5.4 Influencer Culture and Online Persuasion

Pupils will be supported to understand that social media influencers, online personalities and content creators may influence beliefs, behaviours and decision-making.

Teaching will support pupils to:

- Recognise sponsored content and advertising.
- Understand persuasive techniques.
- Consider the impact of influencer culture on body image, wellbeing and self-esteem.
- Make informed and independent decisions online.

6.5.5 Anonymous Messaging and Online Communities

The school recognises that anonymous messaging platforms, online communities and discussion forums can present safeguarding risks.

Potential risks include:

- Cyberbullying.
- Grooming.
- Exposure to harmful content.
- Radicalisation.
- Misinformation.
- Peer pressure and manipulation.

Pupils will be taught how to recognise unsafe situations and seek support when required.

7.0 Cyberbullying and Online Harm

7.1 Types of Cyberbullying and Online Harm

Cyberbullying can take many forms and may occur through social media platforms, messaging services, gaming platforms, livestreaming services, websites, forums or emerging technologies. Examples may include:

Threats and Intimidation

- Threatening messages or comments.

- Threats of violence.
- Threats to share personal information or images.

Harassment

- Repeated unwanted messages.
- Offensive, abusive or discriminatory comments.
- Persistent targeting of an individual online.

Exclusion and Isolation

- Deliberately excluding individuals from online groups or activities.
- Group chat exclusion.
- Coordinated efforts to isolate individuals socially.

Impersonation and Identity Misuse

- Creating fake accounts.
- Accessing accounts without permission.
- Pretending to be another person online.
- Using another person's photos or identity without consent.

Sharing Images or Information

- Sharing private information without consent.
- Screenshotting and distributing private conversations.
- Sharing embarrassing photographs or videos.
- Creating or sharing altered or manipulated images.

AI-Generated Abuse

- Creating or distributing AI-generated images designed to humiliate or distress others.
- Creating deepfake images, videos or audio recordings.
- Using artificial intelligence tools to impersonate individuals or spread misinformation.

Trolling

- Deliberately provoking or upsetting others online.
- Posting inflammatory, offensive or distressing comments intended to cause a reaction.

7.2 Newport Primary School's Approach to Bullying, Cyberbullying and Online Harm

Newport Primary School is committed to providing a safe, inclusive and respectful environment where all members of the school community are valued and treated with kindness. We believe that every child has the right to learn and thrive in an environment free from bullying, discrimination, harassment and intimidation.

Bullying, including cyberbullying and online harm, is not tolerated under any circumstances and will never be dismissed as "banter", "having a joke" or a normal part of growing up. All concerns will be taken seriously and dealt with promptly, fairly and proportionately.

The school promotes a culture of:

- Respect, kindness and empathy.
- Positive relationships and communication.
- Digital citizenship and responsible online behaviour.
- Inclusion and acceptance of difference.
- Personal responsibility and accountability.
- Seeking help and supporting others.
-

Through the curriculum, assemblies, pastoral support and wider school ethos, pupils are encouraged to develop the knowledge, skills and confidence needed to recognise bullying, challenge inappropriate behaviour and seek support when required.

The school uses restorative approaches where appropriate to support pupils in understanding the impact of their actions, repairing relationships and preventing future incidents. Where bullying behaviour is identified, support will be provided for both the child experiencing bullying and the child displaying bullying behaviours.

Newport Primary School is a **telling school**. Pupils, staff, parents and carers are encouraged to report any concerns relating to bullying, cyberbullying or online harm at the earliest opportunity. Pupils are regularly reminded that reporting concerns is the right thing to do and that support will always be available.

The school recognises the importance of strong partnerships between home and school. Parents and carers are encouraged to share concerns promptly so that we can work together to keep children safe and promote their wellbeing.

7.3 Signs of Cyberbullying

- Reluctance to use devices previously enjoyed.
- Increased anxiety around notifications.
- Being unusually distressed after going online.
- Sudden deletion of social media accounts.
- Avoiding online learning or communication platforms.
- Changes in friendship groups.

7.4 Preventing Cyberbullying

The school seeks to prevent cyberbullying through:

- Digital resilience education.
- Online safety education.
- Staff vigilance.
- Positive behaviour expectations.
- Parent engagement.
- Promoting respectful online communication.
- Teaching pupils about consent, privacy and digital footprints.
- Educating pupils about AI-generated content, deepfakes and online manipulation.

7.5 Legality of Cyberbullying

Whilst cyberbullying is not itself a specific criminal offence, some behaviours associated with cyberbullying may constitute criminal offences.

Examples may include:

- Harassment.
- Malicious communications.
- Threatening behaviour.
- Hate-related incidents.
- Sharing intimate images without consent.
- Creation or distribution of indecent images of children.
- Stalking.
- Identity theft or fraud.
-

Where criminal behaviour is suspected, the school may seek advice from or refer matters to the Police and other appropriate agencies.

8.0 Online Gaming

Newport Primary School recognises that online gaming is a popular activity for many children and can provide opportunities for entertainment, creativity, collaboration, communication and problem-solving.

Many modern games include interactive features such as:

- Online multiplayer environments.
- Messaging and group chat functions.
- Voice and video communication.
- Livestreaming and content sharing.
- User-generated content.
- Online communities and forums.
- In-game purchases and subscriptions.

Whilst online gaming can be a positive experience, it may also expose children to safeguarding risks. As part of the school's Digital Resilience curriculum, pupils are taught how to recognise, manage and report these risks appropriately.

8.1 Online Gaming Risks

Pupils are taught about the potential risks associated with online gaming, including:

- Communicating with unknown individuals online.
- Exposure to inappropriate language or content.
- Cyberbullying, trolling and online harassment.
- Grooming and exploitation.
- Pressure to share personal information.

- Livestreaming and gaming broadcasts.
- In-game purchases and spending money online.
- Loot boxes and gambling-style features.
- Scams, phishing attempts and fraud.
- Excessive screen time and unhealthy gaming habits.
- Voice chat and private messaging features.
- The sharing of images, videos or personal information.
- Manipulation by online influencers or gaming communities.

8.2 Safe Online Gaming

Pupils are encouraged to:

- Keep personal information private.
- Use age-appropriate games.
- Follow PEGI age ratings.
- Use privacy and safety settings where available.
- Treat others with kindness and respect online.
- Report inappropriate behaviour, content or contact.
- Speak to a trusted adult if something online makes them uncomfortable, worried or upset.
- Take regular breaks and maintain a healthy balance between online and offline activities.
-

The school promotes the message:

Keep online friends online and speak to a trusted adult if someone asks for personal information or attempts to move conversations to private platforms.

8.3 Supporting Parents and Carers

Parents and carers play an important role in supporting safe online gaming.

The school encourages parents and carers to:

- Familiarise themselves with the games their children use.
- Make use of parental controls and privacy settings.
- Monitor in-game purchases and subscriptions.
- Consider PEGI age ratings when selecting games.
- Discuss online safety and gaming behaviour regularly.
- Establish family expectations around screen time and online conduct.
- Encourage children to report concerns about their online experiences.

Information, guidance and support relating to online gaming may be shared with parents through workshops, newsletters, online safety updates and the school website.

9.0 Sharing Nudes and Semi-Nudes

Newport Primary School recognises that incidents involving the creation, possession or sharing of nude or semi-nude images can occur both online and offline and should always be treated as a safeguarding concern.

The school follows the UK Council for Internet Safety (UKCIS) guidance *Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People* and the procedures outlined within the school's Child Protection and Safeguarding Policy.

The school recognises that incidents involving the sharing of nude or semi-nude images may arise from a range of circumstances, including:

- Peer pressure.
- Curiosity or experimentation.
- Grooming or exploitation.
- Coercion or intimidation.
- Child-on-child abuse.
- Online relationships.
- Criminal or abusive behaviour.

•

Each incident will be considered on its individual circumstances and managed proportionately, with the welfare and best interests of the child being the primary consideration.

9.1 Responding to Incidents

Any incident involving the sharing of nude or semi-nude images must be reported immediately to the Designated Safeguarding Lead (DSL).

Staff should:

- Remain calm and supportive.
- Reassure the child involved.
- Avoid judgemental language.
- Record the concern promptly.
- Follow the school's safeguarding procedures.
- Refer the matter to the DSL without delay.

•

Staff should not:

- Copy, print, share or distribute images.
- Save images to school systems.
- Forward images to others.
- Conduct their own investigation outside safeguarding procedures.

•

9.2 Risk Assessment and Support

Following a report, the DSL will undertake an appropriate risk assessment and determine the most suitable response.

This may include:

- Supporting the child and family.
- Liaising with parents or carers where appropriate.
- Working with Children's Social Care.
- Contacting the Police where necessary.

- Referring concerns to CEOP or other agencies.
- Arranging pastoral or wellbeing support.

9.3 Education and Prevention

Through the Digital Resilience curriculum, pupils are taught in an age-appropriate manner about:

- Respect for themselves and others.
- Consent and personal boundaries.
- Privacy and online reputation.
- Safe online relationships.
- Reporting concerns and seeking help.
- The potential consequences of sharing images online.

The school promotes a culture in which pupils feel able to speak to trusted adults about online concerns and seek help without fear of judgement.

Section 10 – Artificial Intelligence (AI)

Newport Primary School recognises that Artificial Intelligence (AI) presents both educational opportunities and safeguarding challenges. Through the Digital Resilience curriculum, pupils are taught to think critically about AI-generated content, recognise misinformation and manipulated media, and use technology responsibly.

The school will consider AI-related risks as part of its wider online safety, filtering and monitoring arrangements.

Further guidance regarding the use and governance of Artificial Intelligence is contained within the school's Artificial Intelligence (AI) Policy.

11.0 Useful Websites and Support Services

The following organisations provide information, guidance and support for pupils, parents, carers and staff on matters relating to online safety, digital resilience and safeguarding.

Reporting Concerns and Seeking Help

CEOP (Child Exploitation and Online Protection)

For reporting concerns about online abuse, exploitation or grooming.

<https://www.ceop.police.uk>

Childline

Free support and advice for children and young people.

<https://www.childline.org.uk>

NSPCC

Online safety advice and guidance for children, parents and professionals.

<https://www.nspcc.org.uk>

Report Remove

A confidential tool to help young people report and remove sexual images of themselves that have been shared online.

<https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove>

Internet Watch Foundation (IWF)

Report child sexual abuse material and criminally obscene content found online.

<https://www.iwf.org.uk>

Online Safety Education

Childnet

Resources for schools, children, parents and carers.

<https://www.childnet.com>

CEOP Education (Thinkuknow)

Age-appropriate online safety resources and educational materials.

<https://www.thinkuknow.co.uk>

UK Safer Internet Centre

Guidance, resources and support relating to online safety and digital citizenship.

<https://www.saferinternet.org.uk>

Internet Matters

Advice and practical guidance for parents and carers.

<https://www.internetmatters.org>

Be Internet Legends

Educational resources promoting safe and confident internet use.

<https://beinternetlegends.withgoogle.com>

Guidance for Parents and Carers

National Online Safety

Online safety guides, webinars and resources for schools and families.

<https://nationalonlinesafety.com>

Parent Zone

Support for families navigating technology and digital life.

<https://parentzone.org.uk>

Common Sense Media

Reviews, age ratings and guidance on apps, games and digital media.

<https://www.commonsensemedia.org>

Government and Professional Guidance

UK Council for Internet Safety (UKCIS)

National guidance and resources relating to online safety.

<https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Department for Education

Statutory and non-statutory guidance relating to safeguarding and online safety.

<https://www.gov.uk/government/organisations/department-for-education>