



Digital Resilience and E-Safety Policy

The Digital Resilience and E-Safety Policy outlines how Oldcastle Primary School will ensure staff and pupils stay safe online. The Policy should be read in conjunction with the Safeguarding Policy.

Digital Resilience

Oldcastle Primary School aims to support our staff and children to be digitally resilient. Digital resilience is the need to develop knowledge, skills and strategies in order for staff and children to:

- manage their online experience safely and responsibly while protecting their digital identity
- identify and mitigate risks to stay safe from harm online
- understand the importance of using reliable sources and employing critical thinking skills to identify misinformation
- seek help when they need it
- learn from their experiences and recover when things go wrong
- thrive and benefit from the opportunities the internet offers

Building digital resilience in our children will also be dependant on the resilience of our families and communities. We aim to support and inform our families as much as we can.

Our approach to digital resilience focuses on the following:

Well-Being of Future generations

The Well-Being of Future Generations (Wales) Act 2015 aims to tackle the long-term challenges in Welsh communities aiming to create a Wales that we all want to live in, now and in the future.

The Digital Resilience and E-Safety Policy supports the commitment towards addressing the seven well-being goals outlined in the Act, ensuring a collaborative vision and approach.

Building digital resilience within our children will prepare them to become well-rounded and balanced citizens. Ensuring our children use technology responsibly to foster a culture where mental and physical health is not adversely affected by the internet is crucial.

UNCRC - key objective is to support children be responsible citizens

A key aim of our Digital Resilience Policy is to raise awareness of issues that children may encounter online, such as bullying or discrimination (article 2) or sexual exploitation (article 34). The school also pledges to support parents and carers to ensure they understand the use of information technology in school.

Digital Competence Framework

The Curriculum for Wales identifies digital competence as a mandatory cross curricula subject area and we utilise the Welsh Government's Digital Competence Framework across the school. Oldcastle Primary School are committed to developing a robust framework that will develop children and their knowledge of digital resources.

We will teach children:

Citizenship

- Identity image and reputation
- Use of a variety of digital media
- Digital rights, licensing and ownership
- Online behaviour and bullying

Interacting and Collaborating

- Online communication
- Work with others to produce digital work
- Storing and sharing work digitally

Producing

- Sourcing, searching and planning digital content
- Creating digital content
- Evaluating and improving digital content

Data and computational thinking

- Before learners can use computers to solve problems they must first understand the problem and the methods of solving them.
- Collecting data and information.

Oldcastle Primary School is a Google for Education school and will provide children with a range of digital experiences to enhance learning. Pupils in Nursery to Year 1 will have access to a variety of digital resources including iPads. Children in Year 2 will use iPads and learn how to use Chromebooks in readiness for Year 3. Pupils in

Years 3 to 6 will have access to Chromebooks and these are provided on a one to one basis for these children.

Staff in Nursery to Year 2 will use Seesaw to document learning within the classroom. The online platform is a secure site and content is securely managed by Oldcastle Primary School. The Privacy Policy for Seesaw is included on our website.

All children in Years 2 to 6 will be allocated a unique Google log in which is managed by Oldcastle Primary School. Children in Years 5 and 6 will be introduced to Gmail and the school will seek parental permission for children to use Gmail as part of their learning experience. A copy of the Google Privacy Policy can be found on our website.

As part of the Digital Competence Framework the school has developed an overview of Apps / digital tools that should be taught in each year group. This will be reviewed regularly to ensure an innovative curriculum.

Oldcastle Primary School - Digital Apps

Oldcastle Primary School use a variety of digital apps to enhance learning. The apps detailed below are introduced to children as a minimum, additional apps may be introduced as required. Once introduced in specific year groups these will then continue to be utilised by following year groups, this means by Year 6, pupils are using all tools and apps independently.

Nursery	Reception	Year One	Year Two Chromebooks Introduced	Year Three	Year Four	Year Five	Year Six
	J2 Data 	Minecraft 	Google Jamboard 	Google Drive 	Google Sites 	Google Sheets 	
Google (search engine) 	Google Earth 	J2E Folders 	Britannica School/ Britannica Digital Learning 	Google Docs 	Garage Band 	Gmail 	
Beebot/ Bluebot/ Codepilla 	Pic Collage 	JIT5 	iMovie 	Google Forms 			
		J2 Code 	Google Classroom 	Flipgrid 			
		Google Interland 	Google Slides 	J2E5 Multimedia 			
			Adobe Creative 	Stop Motion 			

E-Safety

The internet and other digital technology are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

Oldcastle Primary School will ensure that children are able to use the internet and related digital technology appropriately and safely. This E-Safety Policy should help to ensure safe and appropriate use of these types of technology.

The school E-Safety Policy sets expectations for the safe and responsible use of digital technologies for learning, administration and communication, and describes how the school will help prepare learners to be safe and responsible users of online technologies. The school will:

- regularly review the policy to take into account online safety incidents and changes/trends in technology and related behaviours.
- establish guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should help safeguard learners in the digital world
- help prepare learners to be safe and responsible users of online technologies
- establish clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents
- ensure all staff are aware of this policy at induction and through normal communication channels
- publish the policy on the school website

Social Media

Social networking internet sites provide facilities to chat and exchange information online. The online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact. The following apply in Oldcastle Primary School:

- Use of social networking sites in the school is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- The school will link in with the School Liaison Officer to provide access to information sessions on the use of social media (age dependent)

- Pupils will be encouraged to only interact with known friends, family and staff over the internet and deny access to others.
- All staff are advised not to have contact with children on any social networking site, and be mindful of any contact with parents.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.
- Staff will be made aware of, and adhere, to the BCBC Social Media Policy.
- The school's social media sites will be managed and monitored by the Grants, Media, Health and Safety Manager, Headteacher, and the Deputy Headteacher.
- Only photos of children whose permission has been granted by the parent / carer may be uploaded onto the school social media channels.

Mobile Phones and other electronic devices

Staff should adhere to the Bring Your Own Device and Staff Handbook policy documents on the use of mobile phones.

Pupils are not permitted to carry mobile phones in school. If a mobile phone is bought into school by a pupil this should be handed to the class teacher at morning registration and released at the end of the day.

Staff should not use personal mobile phones to contact parents/carers. School staff will always use the school admin or mobile phone to contact parents/carers.

Staff, including students and visitors, should be mindful when accessing or using their mobile phone within the classroom or on the playground.

Parents cannot use mobile phones on school trips to take pictures of the children.

Staff are allowed to take digital/video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment.

Children should not wear smartwatches to school that can take photographs. The functionality of these watches poses concerns regarding privacy and safety as children are freely allowed to take photos in all areas of the school.

School Website

The school website is a valuable source of information for parents and potential parents. The Grants, Media, Health and Safety Manager will take overall editorial responsibility and ensure the content is accurate and appropriate.

Photographs and videos that include pupils will be selected carefully to ensure parental permission has been obtained. Pupils' full names will not be used anywhere on the website or social media channels, particularly in association with images. Parents may upload pictures of their own children on to social networking sites. If the picture includes another child/children then it is their responsibility to gain permission from that child's parents.

Information System Security

The IT server room will be locked to ensure security of the equipment. Only identified staff will be allowed to access the school server and equipment.

School security systems will be regularly reviewed and BCBC IT protocols will be followed.

The school has a cyber resilience risk assessment in place which will be reviewed regularly.

Data Protection

As a school we place high value on the importance of information security and have a number of procedures in place to minimise the possibility of a compromise in data security. A Data Protection Policy is published on our website.

Related Policies can be found on our website.