REDLAND PRIMARY SCHOOL ONLINE SAFETY POLICY

Reviewed by	Veronika Joy – September 2026
Date of Issue	October 2026
Review Date	September 2027

What is Online Safety?

Online safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's online safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Safeguarding and Child Protection and Data Protection.

Why Is Internet Use Important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and Redland has a duty to provide pupils with quality internet access. Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

How Does Internet Use Benefit Education?

Benefits of using the internet in education include:

- Access to world-wide educational resources including museums, libraries and art galleries
- Rapid and cost effective worldwide communication
- Educational and cultural exchanges between pupils worldwide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of
- Networks and automatic system updates
- Exchange of curriculum and administration data with the Local Authority
- Access to learning wherever and whenever convenient
- Greatly increased skills in Literacy.

How Can Internet Use Enhance Learning?

- The school internet access is designed expressly for pupil use and includes filtering and monitoring appropriate to the age of our pupils.
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Good Habits

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of the online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the provider including the effective management of content filtering.

Dangers To Consider

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyberbullying (this is reported on CPOMS in line with the school's Anti Bullying Policy)
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Inappropriate use of artificial intelligence software (AI), misinformation, disinformation, fake news, conspiracy theories
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to any risks, so that they have the confidence and skills to face and deal with these risks. Redland must demonstrate that we provide the necessary safeguarding to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The online safety policy that follows explains how we intend to do this.

Internet Access and Responsibility

- All staff (including governors) must read and sign the Staff ICT/Laptop Responsible Use Policy before using any school ICT resource.
- Parents are informed that pupils will be provided with supervised internet access.
- If staff or pupils discover unsuitable sites, the URL, time and content must be reported to the computing coordinator who will investigate and take appropriate action, liaising with broadband provider if necessary.

- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email & Online Collaboration

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive messages.
- Pupils must not send emails without permission from a member of Redland staff.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must not access others pupil's accounts or files.
- Whole class or group email addresses should be used in school.
- Pupils must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Pupils must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. As part of the computing curriculum, they will be taught the rules of etiquette for email and will be expected to follow them.
- Pupils must ask permission before accessing the internet and have a clear idea of why they are using it.

Social Networking

- At Redland we block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to invite known friends only and deny access to others.
- Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old.

Use of Artificial Intelligence, Misinformation, Disinformation, Fake News, Conspiracy Theories

At Redland we recognise the valuable potential AI, including generative AI, holds for schools. These include customising learning experiences, preparing high quality resources quickly and supporting educational innovation/creativity. We are aware of the risks posed by AI. These include data

protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations. Our AI policy can be found on our website.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and their risks assessed.
- Mobile phones are not permitted to be used in school by pupils. However, Year 6 pupils are able to bring mobile phones to school but these are to be handed in to the class teacher and stored in a safe place in line with the school's mobile phone policy.
- The sending of abusive or inappropriate text messages or consensual and non-consensual sharing of nude and semi-nude images and/or videos is forbidden.

Published Content & The School Website

- The contact details on the web site should be the school address, email and telephone number. Staff or pupil's personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with our technical support team and broadband provider if necessary.

Protecting Personal Data

Personal data will be processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Further information can be found in the school's Data Protection Policy.

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- These will be logged and dealt with as deemed appropriate by the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

Staff and Parents

- All staff will be given the Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user.
- Parents' attention will be drawn to the Online Safety Policy in newsletters and the school website.