

Rhiwbeina Primary School

E Safety Policy

Rhiwbeina Primary School

E-Safety Policy

Introduction:

The 21st Century has witnessed an exponential increase in the number of children and young people who have embraced new technology as a mode of communication, socialisation, recreation and learning. Technology such as the internet, email, mobile phones and games consoles are now a part of our society and a part of many of our daily lives. The benefits of such technologies are numerous and have changed and shaped the way in which we work, live and communicate with others. But as children of an increasingly younger age begin to use these technologies, there is a recognised need to educate and raise awareness with pupils of the risks, as well as the benefits, of new technologies.

E-Safety encompasses all Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

The improper or unsafe use of technology can present challenges to children, young people, volunteers and staff.

There are a number of key risks to using new technologies, including:

- 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 exploitation and abused 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
- Cyber-bullying
- 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
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Blackmail involving threats to life, dignity and violence.
- Poor or inappropriate supervision of Internet access leading to the viewing of harmful or inappropriate.
- Risk of sexual exploitation

Many of these risks reflect situations in the off-line world and it is essential that this E-safety Policy is used in conjunction with other school policies (eg Behaviour, Anti-bullying and Safeguarding Policies).

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

At Rhiwbeina Primary School we strive to provide the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Teaching and Learning:

At Rhiwbeina Primary School we have a duty to provide our pupils and staff with quality Internet access as part of their learning and teaching experiences. The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and pupils.

It helps to prepare pupils for their on-going learning and personal development needs.

It is a requirement of the Curriculum for Wales and Digital Communication Framework.

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use enhances learning

Internet access is provided by Cardiff Council and designed for pupils. This includes filtering appropriate to the content and age of pupils.

Internet access is planned to enrich and extend learning activities.

Access levels are reviewed to reflect the curriculum requirement.

Pupils are given clear objectives for Internet use and are only able to access the internet if parental consent is given.

Staff select sites which support the learning outcomes planned for pupils' age and maturity.

Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

Pupils are taught how to take responsibility for their own Internet access.

Pupils are taught how to evaluate Internet content

Pupils are taught ways to validate information before accepting that it is necessarily accurate.

Pupils are taught to acknowledge the source of information, when using Internet material for their own use.

Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.

Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Managing Internet Access:

Internet access is provided by Cardiff Council via their school servers and is designed for pupils. The following systems are in place to ensure the safe provision of internet access:

- Cardiff Council provide their own firewall filtering.
- Cardiff Council set Google Safe Search as the default setting within the browser. This option cannot be removed at a local level.
- The school has its own Swurl firewall account allowing us to exclude access to specified websites.
- Our pupil iPads also have a profile which restricts access to age specific apps/videos/media content as well as a profanity and image filter.
- PCs in our Nursery have restricted access to the internet.
- The school's IT coordinator conducts checks to ensure that the filtering methods selected are effective in practice.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Headteacher.

E-mail

Pupils must tell a teacher immediately if they receive an offensive email.

In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.

Pupils are taught not to open suspicious incoming email or attachments.

The forwarding of chain letters is not permitted.

Publishing pupils' images and work

Photographs must not identify individual pupils. Group shots or pictures taken "over the shoulder" are used in preference to individual "passport" style images.

Children's photographs are only allowed to go on the website once written permission has been received from the child's parents.

Children's photographs are not accompanied by names.

Children's work which contains photographs must not also contain the child's name.

Social networking and personal publishing

Pupils will not be allowed to access public chat rooms.

Managing emerging technologies

Mobile phones must not be used during the school day. The sending of abusive or inappropriate text messages is not tolerated.

Staff mobile phones are not used in a school context.

Only school cameras and iPads are used by both staff and children for educational purposes.

Reference – Mobile Phone Policy

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff must not keep confidential information on removable devices such as USB devices unless it is the one provided by the school – Encrypted.

Reference – Personal Data Policy

Policy Decisions:

Authorising Internet access

All staff must read and sign the Acceptable Usage Policy before using any school ICT source.

The school maintains a record of all staff and pupils who have access to the school's ICT systems.

Parents/guardians are asked to sign a consent form regarding their child's internet use (see *Acceptable Usage Policy & Parent Admissions Consent Form*).

Any person not directly employed by the school will be asked to read and sign the "Acceptable use of school ICT resources" before being allowed to access the internet from the school site.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school, nor Cardiff Council can accept liability for any material accessed, or any consequences of Internet access. The school's e-safety policy and its implementation will be monitored and reviewed on a regular basis.

Handling e-safety complaints

Complaints of internet misuse must be referred to the Headteacher.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with the school's Safeguarding Policy.

Pupils and parents are informed of the complaints procedure.

Pupils and parents are informed of the consequences for pupil misuse of the Internet (see *Acceptable Use Policy*).

Communications:

Pupils and the E-Safety Policy

E-safety posters are posted next to all computers so that all users can see them.

Pupils are informed that network and Internet use is monitored and appropriately followed up.

The children receive e-safety lessons and are constantly reminded of online safety.

Staff and the E-Safety Policy

All staff are trained regularly and receive a copy of the e-safety policy.

Staff are informed that network and Internet traffic can be traced to an individual user.

Staff will always use a child friendly safe search engine when accessing the web with pupils. *Google Safe Search*


Parents and the E-Safety Policy

The school has links on its website to e-safety resources for discussion with children

The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.

The E-Safety Policy is reviewed annually.

However, due to the ever changing nature of digital technologies the policy will be reviewed more frequently in response to any significant new developments in the use of technologies, incidents or new threats to e-safety.

Signed  Headteacher Date: September 2023

Signed  Chair of Governors Date: September 2023