E-Safety Policy

Catwg Primary School will allow pupils, staff and appropriate visitors, access to its computers, network services, and the Internet.

E-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people 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 E-safety policy will operate alongside other policies including those for Behaviour, Safeguarding, Curriculum, Social Media and Data Protection.

1. Purpose

The purpose of this policy is to:

- allow users to access the Internet safely for educational purposes
- establish rules for acceptable and safe use of the Internet
- explain the mechanisms in place to protect pupils when working online
- detail how E-safety complaints will be handled

2. Teaching and Learning

The Internet is an essential aspect of 21st century life and is a necessary tool for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Benefits of Internet use include –

- access to a variety of libraries, databases, encyclopaedias, and other sources of information;
- ability to communicate with other Internet users around the world;
- access to up to date news and current affairs;

Internet access will be planned to enrich and extend learning. Pupils will -

- learn about acceptable Internet use and made aware of what is unacceptable
- take part in e-safety programmes through the PSE curriculum and the All Wales School Liaison Core Programme delivered by South Wales Police
- be given clear objectives for Internet use
- be supervised appropriately
- learn how to use the Internet for research
- be taught to be critical of the materials on the Internet and shown how to validate information before accepting it as accurate

3. Good Practice

E-safety depends on effective practice at a number of levels:

- responsible ICT use by all staff and pupils.
- implementation of E-safety policy in both administration and curriculum.
- provision of a secure school network infrastructure by the Local Authority, including the effective management of content filtering.

4. Authorised Internet Access

All staff must read and sign the Acceptable Use Policy before using any school digital devices.

Parents will be informed that pupils will be provided with supervised e-mail and Internet access and will be asked to give written content for this access.

5. Acceptable Use

Users are expected to use the network systems responsibly. Examples of unacceptable use include but are not limited to the following:

- users must not download software without approval from the ICT co-ordinator
- accessing or creating, transmitting, displaying or publishing any material that is likely to cause offence or anxiety to others. (the county council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)
- accessing or creating any defamatory material
- receiving, sending or publishing material that violates copyright law
- receiving, sending or publishing material that violates the data protection act
- unauthorised access to data and resources on the school network system or other systems.
- any action that would destroy other users' data, or violate the privacy of other users

6. Responsible Use

- pupils are responsible for appropriate behaviour on the school's computer network just as they are in the classroom or on the school playground.
- staff may review documents and log files to ensure that pupils are using the system responsibly.
- pupils should never download, load or install any material without seeking permission
- pupils must not access the files of other pupils without permission
- abusive or rude language must never be used whilst accessing the school network
- if pupils come across any material they are unsure about, they should immediately report it to their teacher.

7. General Personal Security Guidelines for Internet and E-mail use

Pupils should -

- not reveal personal details of themselves or others
- not arrange to meet anyone without specific permission of teachers or parents/guardians
- be made aware that someone contacting them may not be the person they claim to be
- not use photographs of themselves unless parents/guardians/teachers have given permission to do so
- notify their teacher whenever they come across information or messages that are inappropriate, or make them feel uncomfortable

8. E-mail

- pupils may only use approved e-mail accounts on the school system
- staff will make initial email contact
- pupils must immediately tell a teacher if they receive offensive e-mail
- the forwarding of chain letters is not permitted

9. Social Networking

Access to social networking sites is blocked. Pupils are advised that the use of social networking sites outside of school is inappropriate for primary aged pupils.

10. School Website and Twitter Account

- contact details on the website will be the school's, the personal information of staff/pupils will not be published
- photographs which include pupils will be carefully selected and won't include full names of pupils unless permission is given
- written permission from parents/carers will be obtained before photographs or video footage are published
- the Headteacher will have overall editorial responsibility for ensuring that content is appropriate

11. Security

The school will take all reasonable precautions to ensure that users access only appropriate material.

The IT system used at Catwg Primary School is provided by the Local Authority through a managed service. Internet content is filtered and use is monitored. This means that pupils only view internet content that has been identified as appropriate.
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 school device. Neither the school nor NPT Council can accept liability for any material accessed or any consequences of Internet access.

Virus protection is regularly updated.

All Internet activity is logged via the Local Authority's managed service. Any unsuitable content should be reported to the Headteacher.

Access to the internet is through confidential passwords. Passwords should never be shared.

Staff and pupils should be discouraged from using removable disc storage and should store their work on the managed service system. If removable storage devices are used eg memory sticks, these should be password protected.

12. E-Safety Complaints

Any complaints related to E-safety should be referred to the Headteacher.

Complaints of a child protection/safeguarding nature must be dealt with in accordance with the relevant school procedures.