St. Mary's Catholic Primary School

Love, Grow, Believe, Achieve!

E-Safety Policy

Issue	Author	Date
1.0	LA Model Policy/ C Russell	July 2022

Introduction

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The policy relates to other policies including ICT, Anti-Bullying, Child Protection and Health and Safety.

Use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the improper or unsafe use of technology can present challenges to children, young people, volunteers and staff. The aim of this policy is to ensure a consistent approach across the school to minimising risk and educating children and staff in matters relating to the safe use of the IT and the internet.

Some of the potential risks could 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 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.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / 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.

Writing and Reviewing the e-Safety Policy

The school has a designated e-safety co-ordinator – Claire Russell

The e-Safety policy will be agreed by the senior leadership team and approved by the governors. It will be reviewed on a regular basis or as necessary if an incident occurs.

Teaching and Learning

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 students. It helps to prepare students for their on-going career and personal development needs. It is a requirement of Digital Curriculum Framework as part of the Curriuclum for Wales.

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 and access levels are reviewed to reflect the curriculum requirement. Pupils are given clear objectives for Internet use. Staff select sites which support the learning outcomes planned for pupils' age and maturity. 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

Information System Security:

- School ICT system security is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with the Local Authority.

E-mail:

- Pupils are allowed to use Hwb email accounts only.
- Pupils must tell a teacher immediately if they receive 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.

Published content and the school web site:

- The website complies with the school's guidelines for publications.
- Pupils are taught to consider the audience and purpose for the work they publish on the school website and ensure their work is of high quality.
- All material must be the author's own work or where permission to reproduce has been obtained, it is clearly marked with the copyright owner's name.
- The contact details on the website are for school admin only.

Publishing pupils' images and work:

- Photographs must not identify individual pupils’ names. 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 social media or used in documents 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.

Managing filtering:

The school works in partnership with parents, the LA, Welsh Government, and the Internet Service Provider to ensure filtering systems are in place to protect pupils and that these are reviewed and improved. Appropriate filtering is set up by the LA to ensure pupils are safe from extremist material.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Headteacher or Digital Lead.

Managing video conferencing and webcam use:

Video conferencing uses Hwb Office 365 Teams and pupils must follow the school's Behaviour Policy. Video conferencing is always appropriately supervised and pupils must ask permission before accepting or making any calls.

Managing emerging technologies:

Mobile phones must not be used during lessons. The sending of abusive or inappropriate text messages is forbidden. Cameras in mobile phones are not used by staff or pupils. Only school cameras are used by both staff and children for educational purposes.

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 suitably security protected.

Policy Decisions

Authorising Internet access:
The school maintains a record of all staff and children who have access to the school's ICT systems. Parents are asked to sign a consent form regarding their child's internet use (see Acceptable Use Policy).

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 child protection policy.
- Pupils and parents are informed of the complaint's procedure.
- Pupils and parents are informed of the consequences for pupil misuse of the Internet (see Acceptable Use Policy).

Community use of the Internet:
The school liaises with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils:

- 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.

Enlisting parents' and carers' support:

- Parents' and carers' attention is drawn to the school's E-safety Policy in newsletters, the school brochure and on the school website.
- The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.