

**SACRED HEART CATHOLIC PRIMARY SCHOOL  
HINDLEY GREEN**



*Grow in the Spirit of Love and Learning*

# **E-Safety Policy**

ADOPTED BY GOVERNORS ON:

28<sup>th</sup> June, 2018

REVIEW DATE:

June, 2020

**Our Mission**  
**“Grow in the spirit of love and learning”**

Our Mission is to put our Catholic faith at the centre of everything we do to value and respect each individual

to inspire a love of learning

harness a natural curiosity to develop a thirst for knowledge

to prepare our children for opportunities and responsibilities in the adult world

to share our talents at the heart of the local and wider community

*Finally we will **cherish** the Christian values of forgiveness, love, care and respect for others, especially the more vulnerable, encouraging a love of learning and a zest for life.*

### **Safeguarding Children**

Sacred Heart Catholic Primary school is committed to providing a safe and secure environment for children, staff and visitors and promoting a climate where children and adults will feel confident about sharing any concerns which they may have about their own safety or the well-being of others. We aim to safeguard and promote the welfare of children by protecting them from maltreatment; preventing impairment of children’s health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.

The School’s Safeguarding policy draws upon duties conferred by the Children Acts 1989 and 2004, The Children and Families Act 2014, S175 of the 2002 Education Act, and the guidance contained in “*Working Together to Safeguard Children*”, the DfE’s statutory guidance “*Keeping children safe in education*”, Guidance and procedures produced by the Wigan Safeguarding Children Board. We also have regard to the advice contained in DfE’s “*What to do if you’re worried a child is being abused*” and “*Information Sharing – Advice for practitioners*”. The policy is applicable to all on and off-site activities undertaken by pupils whilst they are the responsibility of the School.

### **Learning**

#### **1. Why the Internet and digital communications are important**

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with high-quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

## **2. Internet use will enhance and extend learning**

Staff will be made aware of and pupils will be educated in the safe use of the internet. Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the Internet and digital communications.

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

## **3. Pupils will be taught how to evaluate Internet content**

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## **Managing Internet Access**

### **1. Information system security**

School ICT system security will be reviewed regularly.

Virus protection will be installed and updated regularly.

### **2. E-mail**

Pupils and staff should only use approved curriculum e-mail accounts at *schoolomain.wigan.sch.uk*

Pupils must be made aware of how they can report abuse and who they should report abuse to.

Pupils must report if they receive offensive or inappropriate e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school should consider recommending a standard mail format for all users.

The forwarding of chain letters is not permitted.

### **3a Published content and the school web site**

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

The head teacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

### **3b Published content**

Staff or pupil private and personal contact information will not generally be published. The contact details provided will be the person's official curriculum e-mail address

#### **4. Publishing students' images and work**

Photographs that include pupils will be selected carefully so that images of individual pupils cannot be misused.

Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Written permission, using the approved permission form, from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Work can only be published with the permission of the pupil and parents/carers.

#### **5. Social networking and personal publishing**

The school will educate people in the safe use of social networking sites, and educate pupils in their safe use.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils must be made aware of how they can report abuse and who they should report abuse to.

Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.

Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

#### **6. Managing monitoring and filtering**

The school will work in partnership with Wigan Council and Becta to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Lead or the Network Manager.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

#### **7. Managing emerging technologies**

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The senior leadership team should consider in their policy making that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Where contact with pupils is required to facilitate their learning, staff will be issued with a school phone.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

It should be noted that games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

## **8. Protecting personal data**

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

## **Policy Decisions**

### **1. Authorising Internet access**

All staff must read and sign the 'Staff Acceptable Use Policy and Code of Conduct for ICT' before using any school ICT resource, including any laptop issued for professional use.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Parents/carers will be asked to sign and return a consent form.

### **2. Assessing risks**

The school will take 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 Wigan Council can accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective.

Schools must ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

### **3. Handling E-Safety complaints**

Complaints of Internet misuse will be reported to the E-Safety Lead and action in-line with the Wigan Safeguarding Children Board E-Safety policy will be taken.

Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the LADO within one working day in accordance with Wigan Safeguarding Board policies.

Any complaint about staff misuse must be referred to the head teacher and if the misuse is by the head teacher it must be referred to the chair of governors in line with Wigan Safeguarding Board Child Protection procedures.

Pupils, parents and staff will be informed of the complaints procedure.

## **Communicating E-Safety**

### **1. Introducing the E-Safety policy to pupils**

E-Safety rules will be posted in all rooms where computers are used.

All system users will be informed that network and Internet use will be monitored.

A programme of E-Safety training and awareness raising will be put in place in-line with the Wigan Safeguarding Children Board's E-Safety Strategy.

### **2. Staff and the E-Safety policy**

All staff will be given access to the School E-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops.

Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

### **3. Enlisting parents' and carers' support**

Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.