Holy Family Catholic Primary School, New Springs

Mission Statement
We are a caring family, we pray, learn and grow together

E-Safety Policy

Writing and reviewing the E-Safety Policy

- The E-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The school has an appointed E-Safety Lead who works alongside the Designated Child Protection Officer.

- Our E-Safety Policy has been written by the school, building on the Wigan Safeguarding Childrens Board (WSCB) E-Safety strategy and government guidance. It has been agreed by staff and approved by governors.

Learning

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.

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.

Pupils will be taught how to evaluate Internet content

- We will 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

Information system security

- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be used as recommended by the Local Authority –Securus.

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.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff laptops and iPads must be encrypted and/ or password protected when transported outside school.
- Personal pupil information must not be stored on personal pen drives.

Policy Decisions

Authorising internet access

- All staff must read and sign the 'Guidance for Schools on Acceptable Usage of IT' and 'Staff Code of Conduct' 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.
- External partners / contractors / colleagues visiting school on official business and requiring the internet may connect their laptop / mobile device to the school curriculum wireless network with permission from the headteacher or his representative. They should be made aware that Securus will monitor their access during the time they are connected.

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.

Handling E-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 Headteacher. Pupils, parents and staff will be informed of the complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communicating E-Safety

Introducing the E-Safety Policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

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. Discretion and professional conduct is essential.
- Staff are not permitted to use their own personal phones or devices to contact children, young people and their families within or outside the setting in a professional capacity. Staff will be reminded to use the phone in the school office for such communications. Mobile phones and devices must be out of sight (e.g. in a drawer or handbag) during class time and switched off or switched to silent mode with Bluetooth communication being "hidden" or turned off. Under no circumstances must mobile phones be used during teaching periods and in the presence of children. Staff must never use mobile phones or personal cameras to take photos or videos of pupils and will instead only use work-provided equipment for this purpose. If a member of staff breaches the school policy then disciplinary action may be taken.

Social Networking Sites like Facebook / Twitter / MSN

- Staff will not add children from school as their friends on any social networking site.
- Staff will not discuss professional activities that identify school, individuals employed by or attending school or private/ confidential school matters on social networking sites. In particular staff are reminded that any negative comments posted and available for others to see may result in disciplinary action.
- Staff will not post photographs of school or children from school on personal social networking sites. Staff can only post such material on the approved schools website and social networking sites and with the appropriate parental consent.
- Staff will block and not reply to children requesting to be their friends on any social networking site.
- Staff are reminded to take care to secure their own social networking profiles and to consider carefully who they add to their friends lists, particularly any friends whose children also attend this school.
- Staff are at liberty to mention where they work on social networking sites but are reminded that this could put them at risk if the information is not secure.
- Staff are encouraged to carefully set the privacy and security settings on their online profiles so as to safeguard themselves and ensure children from this school cannot find them easily.
- Staff will not use school equipment or the school internet to access social networking sites.

Professional Social Networking Sites such as LinkedIn

- Staff are at liberty to use professional social networking sites. School recognises that this is now seen as a good way to find new jobs, keep up to date with new ideas and be seen on the professional scene.
- Staff are reminded that when they network on professional social networking sites and make reference to school or school activities, they represent the school. As such, professional behaviour and attitudes are therefore important so as not to bring the school into disrepute.
- Inappropriate behaviour on professional networking sites that affects school in any way may result in disciplinary proceedings.
- Staff are reminded that they should secure their personal profiles on professional networking sites in the same way as they would with personal social networking sites. Not everyone is who they say they are.
- Staff are reminded that information that is online in the public domain can be very difficult to remove and can be manipulated, copied and used in unexpected ways. They should think very carefully about what they post because once it is available publicly, it can be very difficult, if not impossible, to remove and this may have serious personal implications in the future.
- As it may be necessary for staff to communicate online with other educational professionals during the school working day, staff may use the school internet to access professional networking websites with the permission of the headteacher.

.

E-mail

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

.

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 by the school office.
- The headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

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 Website or other on-line space 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 website.
- Work can only be published with the permission of the pupil and parents/carers.

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 whom 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.

Managing monitoring and filtering

- The school will work in partnership with Wigan Council 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.
- Monitoring software called Securus is used to monitor usage of the school curriculum computers and network. Securus captures records of misuse and unacceptable behaviour, such as swearing, accessing inappropriate or filtered websites and explicit images and identifies the user involved. Securus covers all internet use, all software, teachers' laptops, all websites, email, use of chat, forums and other social networking sites. All inappropriate use, misuse or abuse is reviewed by senior staff, who then decide on the action to be taken.
- The school curriculum network is filtered through the Wigan Council filtering system.

Policy reviewed Spring 2019