



# Ysgol yr Holl Saint All Saints' School



## E-Safety & Social Networking Policy

Equality Act Impact Assessment	YES	NO	March '19
Last Review Date	N/A		
Date to be reviewed by Senior Management Team	February 2025		
Date Adopted by Governing Body	14.03.2023		
Head Teacher - Mr Richard Hatwood			
Chair of Governors - Father Tudor Hughes			



## **Introduction**

This E-Safety & Social Networking Policy is a central part of the approach taken by the school to ensure the safe and appropriate use of technology as a tool to enhance teaching and learning. It links closely to several other policies including those for ICT, anti-bullying and for Child Protection and Safeguarding.

- The school will appoint an e-Safety Coordinator. This will be the Designated Child Protection and Safeguarding Officer as the roles overlap. It is not a technical role.
- Our e-Safety Policy has been written by the school, building on the Local Authority E-Safety Policy and government guidance. It has been agreed by Senior Management Team and approved by governors.
- The E-Safety and Social Networking Policy and its implementation will be reviewed regularly.

## **Teaching and 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 and staff with relevant digital learning opportunities as part of their learning experience.
- Internet use is a part of the statutory educational curriculum and is a necessary tool for staff and pupils.

### **Internet use will enhance teaching and learning**

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 shown how to publish and present information to a wider audience.

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

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

## **Managing Internet Access**

### **Information system security**

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

### **E-mail**

- Messages sent using the schools email system should not be considered private and the school reserves the right to monitor all emails.
- Pupils may only use Welsh Government approved e-mail accounts on the school system.
- Whole-class or group e-mail addresses will be used in most situations.
- Pupils must immediately tell a teacher 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 how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

### **Published content and the school website**

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual pupils.
- 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 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.
- Pupil image file names will not refer to the pupil by name.
- Parents/carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

## **Social networking and personal publishing**

- Wrexham IT department will, by default, block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Members of staff will not engage in dialogue about the school or with parents through the use of social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will not be able to use social networking sites in school.
- Pupils and parents/carers will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites as part of their ongoing education for out of school use.

## **Managing filtering**

- The school will work in partnership with WCBC IT Department and the Education and Early Intervention ICT Service to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the web site address and a description of the inappropriateness of its content must be reported to the schools e-Safety Coordinator and the person responsible for monitoring filtering.
- If staff or pupils come across on-line material which is believed to be illegal (e.g. child pornography), the computer will be quarantined – its power removed and physically secured from tampering. Details will be reported immediately to the E-Safety Coordinator and headteacher and Wrexham IT department notified. Outside agencies such as the Police will be informed as appropriate.
- The filtering service provided by the IT Department protects staff and pupil computers from viruses and intrusive material, e.g. spy-ware. To further protect staff and pupil computers a suitable anti-virus product which is kept up-to-date is installed on all computers used for Internet access.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If a web site or part of a web site is blocked by the Internet security systems which the school believes staff and/or pupils should have access to, details of the web site and a description of why access is requested will be passed to the Wrexham IT department Help Desk by the person responsible for monitoring filtering in the school.
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by the Wrexham IT department.

## **Managing videoconferencing & web cameras**

- Video conferencing should use the educational broadband network to ensure guaranteed quality of service and security.
- Pupils must ask permission from the supervising teacher before using a webcams.
- Any faults with Videoconferencing equipment should be reported to the IT Department Helpdesk who will assign an appropriate technician to resolve any faults.
- Videoconferencing and web camera use will be appropriately supervised for the pupils' age.

## **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 sending of abusive or inappropriate text messages or files by any means is forbidden.
- Mobile phones will not be used during lessons or formal school time.
- The use by pupils of mobile phones, cameras and music players will be kept under review.
- The appropriate use of Learning Platforms such as Hwb will be monitored closely by staff to ensure Blended Learning has the desired impact on teaching and learning.

## **Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the GDPR Regulations 2018.

## **Policy Decisions**

### **Authorising Internet access**

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- In the Foundation Phase access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Pupils will be asked to sign the school's "E-Safety Rules" consent form along with their parents or carer's.
- Any person not directly employed by the school will be asked to sign and agree to 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site. This will include Teaching Trainees and official voluntary helpers.

### **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 Wrexham County Borough Council can accept liability for any material accessed, or any consequences of Internet access.
- The school will 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 will be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

## **Communications Policy**

### **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.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed making best use of Welsh Government tools and resources and those from the School Police Liaison Officer.
- E-Safety training will be embedded within the curriculum through use of the Digital Competence Framework.

### **Staff and the e-Safety policy**

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- 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 will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

## **Evaluation & Review**

This policy will be reviewed by the Senior Management Team and Governing Body and adopted by the Governing Body as per the schedule on the front page.