Saint Ambrose Barlow Catholic Primary School

E- Safety Policy 2021-22

Introduction

At St. Ambrose Barlow Catholic Primary School, the use of the internet and technology is an integral part of the school. The internet is used as a tool to engage the children in their own learning and enable them to use the world wide resources. The statutory curriculum requires pupils to learn how to use technology safely and respectfully, keeping personal information private. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning, such as touch screen tablet devices. Computer skills are vital to access life-long learning and employment; indeed, computing is now seen as an essential life-skill ensuring each child is at a level suitable for the future workplace. It is vital that the children are kept safe at all parts during their school and that they learn lessons that help them keep safe outside too. This e-safety policy is designed to ensure that school, parents and pupils within it are safeguarded and taught how to keep safe not only in school but to transfer this to internet use in the home, library or on mobile devices. Also, within this policy it outlines the importance of making sure clear and appropriate measures are in place if any child or adult feels this is not the case.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible computer use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband via the Local Authority;
- A school network that complies with the National Education Network standards and specifications.

There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Why is the internet an important resource?

· 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 quality Internet access as part of their learning experience.
· The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well being and to support the professional work of staff and to enhance the school's management information and business administration systems.

How will the internet be used to enhance learning?

On a basic level, children need to be aware of the internet and its uses, and through this gain a understanding of how to use it effectively and safely. Through the use of this children will learn to recognize acceptable and unacceptable behavior and identify ways to report concerns about its use and content. To ensure this

- The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
- Pupils will be taught how to effectively review the content they view and a range of ways to report its content.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator will ensure that system capacity is reviewed regularly by Leapfrog.
- The use of user logins and passwords to access the school network will be enforced.

How will e-mail be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

- Whole -class or group email addresses will be used for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

How will published content be managed?

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Staff will use group photographs rather than full-face photos of individual children.
- 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. (this will be covered in the parental letter signed, by parents, at the beginning of each academic year)
- 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.

Social networking and personal publishing

- The school will not allow social networking sites to be used within school.
- The school will ensure pupils are aware of dangers of using social networking sites outside of school.
- 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.

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.

Managing videoconferencing

- Videoconferencing should use the Wigan Video Conferencing Network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be supervised at all times.

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 note 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.
- Pupils' mobile phones are not allowed in school.
- The use by pupils of cameras in mobile phones is forbidden.
- 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.
- Staff will use the school phone where contact with pupils/parents is required and not their own mobiles.

Protecting personal data

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

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 not granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resource before being allowed to access the internet from the school site.

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 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 must be referred to the Head teacher.
- 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.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

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.
- E-Safety training will be embedded within the Computing Curriculum work and the Personal Social and Health Education (PSHE) curriculum.

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 prospectus and on the school Web site.
- The school will ask parents to sign the parent /pupil agreement at the start of each academic year.

Our School Policy has been agreed by the Senior Leadership Team and approved by governors. This policy will also be included and is part of the Child Protection Policy. The children will be aware that they can contact any member of staff regarding any e-safety issue should it arise, however, this information will be passed to both the Child Protection and ICT Coordinator.

The School e-Safety Coordinator is ……
Policy approved by Head Teacher: ……

Policy approved by Child Protection ……..
Date: ……
Policy approved by Governing Body: ……..(Chair of Governors)
Date: ……

The date for the next policy review is September 2022.

Web-based Resources

For Schools

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

KidSmart http://www.kidsmart.org.uk/
SMART rules from Childnet International and Know It All for Parents

Childnet International http://www.childnet-int.org/
Guidance for parents, schools and pupils

Becta http://schools.becta.org.uk/index.php?section=is
e-Safety Advice

Becta / Grid Club, Internet Proficiency Scheme
On-line activities for Key Stage 2 pupils to teach e-safety.
http://www.gridclub.com/teachers/t_internet_safety.html

DfES Anti-Bullying Advice http://www.dfes.gov.uk/bullying/

Grid Club http://www.gridclub.com/teachers/t_internet_safety.html

Internet Watch Foundation www.iwf.org.uk
Invites users to report illegal Websites

Think U Know www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

For Parents

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

Childnet International http://www.childnet-int.org/
"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help
their children stay safe online.

Saint Ambrose Barlow Primary School

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

· I will ask permission before using the Internet.

· I will use only my class network login and password, which is secret.

· I will only open or delete my own files.

· I understand that I must not bring into school and use software or files without permission.

· I will only e-mail and open attachments from people I know, or my teacher has approved.

· The messages I send will be polite and sensible.

· I understand that I must never give my home address or phone number, or arrange to meet someone.

· If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

· I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.

· I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.