E-safety Policy

Mission Statement

This is our school St Werburgh's and St Columba's

A place to be inspired, be accepted, be yourself and be unique.

Be able to grow spiritually, academically and morally.

Be able to contribute to the community and be a responsible global citizen.

Be able to reach for the stars and fulfil your potential.

A place, providing an excellent Catholic education for everyone.

Where we belong, where everyone belongs.

Action Summer 2021

Review Autumn 2024

The policy was written in April 2021 by the Technology Leader, and the Safeguarding Lead will be reviewed annually by the Technology Leader each Summer term. In addition, the policy is approved by the Teaching and Learning Committee every two years. Next review Summer Term 2024.

Aims and expectations

It is a primary aim of our School that every member of the school community feels safe. Therefore, the school e-Safety policy is designed to support the way all members of the school community can use ICT and technology safely both at home and in School. It aims to promote an environment where everyone feels safe and secure.

The primary aim of the e-Safety policy is to educate children and parents on how to use ICT safely and appropriately. In addition to the Internet, it also includes electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to control their online experiences. The School's e-safety policy will operate in conjunction with other policies, including Pupil Behaviour and anti-bullying.

1 Teaching and learning

Why is Internet use essential?

- The Internet is an essential element in 21st-century life for education, business and social interaction. Therefore, the School must provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning
- The school Internet access will be designed expressly for pupil use and include filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

• Pupils are 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

• The School will ensure that staff and pupil's use of Internet-derived materials comply 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.

2 Managing Internet Access Information system security

• School ICT systems capacity and security will be reviewed regularly.

• Virus protection will be updated regularly.

• Security strategies will be discussed with Cheshire West and Chester Authority

E-mail

• Pupils are not permitted to use email accounts on the school system

• Pupils must immediately tell a teacher if they receive offensive e-mail

• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone

Published content and the school web site

• The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

• The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

• Pupils' full names will not be used anywhere on the Web site or Blog, 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.

Social networking and personal publishing

• The School will block/filter access to social networking sites.

• Newsgroups will be blocked unless a specific use is approved.

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

• Pupils and parents will be advised that social network spaces outside School are inappropriate for primary aged pupils.

Managing to filter

• The School will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

• If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator at ICT unit, Cheshire West & Chester Council

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

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.

• Mobile phones will not be used by anybody in School during lessons or formal school time. In addition, the sending of abusive or inappropriate text messages is forbidden.

• Staff will use a school phone where contact with pupils is required.

Protecting personal data

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

3 **Policy Decisions Authorising Internet access**

• All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

- The School provide internet access for all staff and pupils. We subscribe to software which enables School to review internet usage and sites visited. If any use contravenes our policy, staff and pupils access can/will be withdrawn

• The School will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance, a staff member may leave or a pupil's access be withdrawn.

• At Key Stage 1, access to the Internet will be by adult demonstration and supervised access to specific, approved online materials.

Assessing risks

• The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer.

• The School will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is 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

• Complaints of a child protection nature must be dealt with according to the School's child protection procedures.

• Pupils and parents will be informed of the complaints procedure

• Discussions will be held with the local police schools liaison officer Sally-Anne Malone to establish procedures for handling potentially illegal issues.

Community use of the Internet

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

4 **Communications Policy**

Introducing the e-safety policy to pupils

• E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.

• Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

• All staff will be given the School e-Safety policy and its importance explained.

• Staff should be aware that Internet traffic can be monitored and traced to the individual

user. Discretion and professional conduct are essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site. We will hold E-Safety Workshops for parents. On the school website, information is posted regarding the safe use of the Internet and other technology.

Failure to Comply

Failure to comply with this policy will be considered a severe risk to health & safety, and a senior member of staff will investigate all incidents of non-compliance.

Non Statutory Policy

Staff Acceptable Use Agreement / Code of conduct

Use of Facilities

All uses, whether for private or official purposes, in or outside the work place, must observe

• The law

• Financial regulations and codes of practice on financial management

• Terms of employment

• Information Security Policy and Acceptable Use Policy including Data Protection

It is not acceptable to use school equipment and materials or an employee's own equipment/materials in the workplace in any of the following contexts:

• Illegal activity

• Activities for private gain

• Personal shopping

• Excessive personal messages

• Playing games (except where forming part of educational activity)*

• Gambling

• Political comment or any campaigning

• Personal Communications to the media

• Use of words or visual images that are offensive, distasteful or sexual explicit

• Insulting, offensive, malicious or defamatory messages or behaviour

• Harassment or bullying

• Random searching of the web other than for curriculum or professional development purposes

• Accessing sites that could be regarded as sexually explicit, pornographic or otherwise distasteful or offensive.

• Using special web search facilities to disguise actual sites visited

• Using message encryption except where this is required for official school business purposes.

• Racist, sexist or other conduct or messages, which contradict the Council (adopted by the School) employment diversity policies.

• Actions that could embarrass the Local Authority and School or bring it into disrepute. Reference should also be made to the Information Security Policy and Staff ICT Acceptable Use Policy

*Except those games preloaded as part of the Microsoft programme suite, which may be accessed in the employees own time.

If any staff member inadvertently accesses an inappropriate website they should leave it immediately but notify their Headteacher of the incident giving the date and time, the web address (or general description) of the site and the action taken.

COVID 19 ADDENDUM March 2020

This addendum should be read in conjunction with the following policies

- School Behaviour Policy
- Anti Bullying Policy
- Safeguarding Policy
- Staff ICT Acceptable Use Policy

- Information Security Policy

Due to the switch to remote learning during the period of school closure, certain principles not included in these policies need to be adhered to.

Staff/ Pupil/ Parent Communication

- All online communication with parents should be via email with answers and emails sent via the admin email account
- No other messaging tool should be utilised e.g. messenger, What's App, Facebook etc.
- Communications should always be formal and written professionally.
- Any posting of content on social media e.g. school twitter account and PTA Facebook account, must be sent to the Headteacher for checking before posting. Remember - please be mindful of posting on your personal profiles, School in a professional capacity still employs you
- No personal detail of pupils should be shared on Twitter of Facebook only their first names for instance if sharing a piece of work.
- Use of any online conferencing facilities with children or parents should be checked with C Wyna prior to being arranged or undertaken.

Reporting Concerns

- Pupils will be encouraged to raise any concerns they have regarding safeguarding on Toot Toot.
- All staff should utilise Toot Toot to log concerns, and if required, contact the Designated Safeguarding Leads K Oates and K Prendergast. If not on site, they can be contacted by telephone. K Oates 07813318807 K Prendergast 07437313714
- Toot Toot will be monitored by K Oates and K Prendergast

Remote Learning guidance support for pupils and parents

- Apps used by staff to set work for pupils should be ones already used in School, and if new resources are being utilised, they must be vetted before posting for suitability.