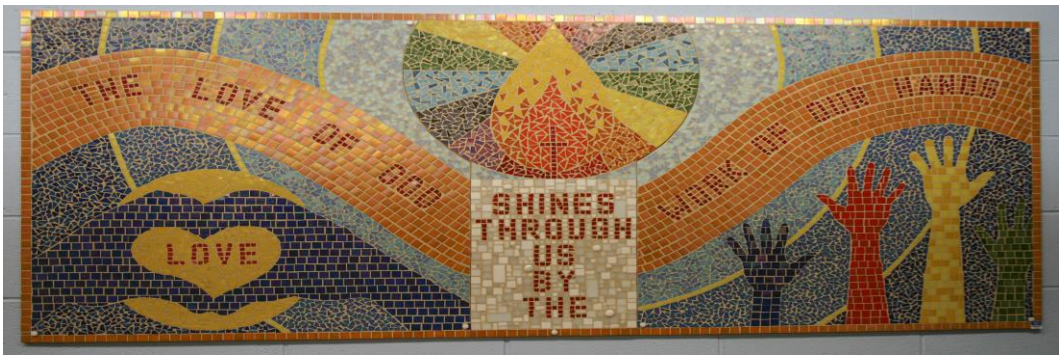
Norley CE Primary School



E-Safety Policy

We are a church school where education is nourished through the teachings of Jesus Christ, enabling each child to fulfil their potential and which reflects our commitment to academic excellence.

We want our children to celebrate and appreciate diversity, fostering qualities that encourage every child to have aspiration for a society in which every individual is cherished.

With our Christian belief at its heart, we work in partnership with each other, families, the church, the local and wider community to create a stimulating and caring environment, where everyone is welcomed, nurtured and empowered.

Christian values directly inspire and influence the children to recognise their self-worth and flourish, enabling them to make the right choices that will continue to shape their lives.

You are the light of the world. A city built on a hill cannot be hidden. No one after lighting a lamp puts it under the bushel basket, but on the lamp stand, and it gives light to all in the house. In the same way, let your light shine before others, so that they may see your good works and give glory to your Father in heaven.
(Matt. 5:14-16)

E-Safety Policy

Introduction

E-safety encompasses the use of new technologies, internet and electronic communications such as learning platforms, mobile phones, video conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-safety depends on effective practice at a number of levels:

- Responsible ICT (Information & Communication Technologies) use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from an approved Internet Service Provider using suitable filtering.
- National Education Network standards and specifications.

Our E-Safety Policy and its implementation is updated on an annual basis. Our E-Safety Policy has been written in conjunction with staff at school, building on the Cheshire E-Safety Policy and government guidance. It has been agreed by senior management and approved by governors. It will be shared with parents/carers.

Our e-safety coordinator is:

- Mrs Kelly

The coordinator works closely with the Local Authority (LA), the school's nominated broadband and filtering service and the school's nominated ICT support provider.

Key LA contacts:

- Cheshire Safeguarding Children in Education Service (SCiE)

Preventing Extremism and Radicalisation

Our Preventing Extremism and Radicalisation policy is intended to provide a framework for dealing with issues relating to vulnerability, radicalisation and exposure to extreme views. We recognise that the internet and in particular social media are used to radicalise and recruit young people. This policy should be read in conjunction with our Preventing Extremism and Radicalisation policy and the Home Office publication 'How Social Media is used to encourage travel to Syria and Iraq- briefing note for schools.' (July 2015).

In the same way teachers are vigilant about signs of possible physical or emotional abuse in any of our pupils, any concerns for the safety of a specific young person at risk of radicalisation are dealt with using the schools safeguarding procedures. We have a Prevent lead who can also provide support.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide students 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 and family use and will include filtering appropriate to the age of pupils.
- Pupils and families 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 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 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

i. Information system security

- School ICT systems and security will be reviewed regularly.
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily
- We have adopted Cheshire West and Cheshire's security standards

ii. E-mail

- Pupils may only use approved e-mail accounts on the school system. The School does not permit individual pupils to have their own email accounts. Accounts are set up on a class basis.
- 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 without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

iii. Published content and the school website

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

- The headteacher will take overall editorial responsibility for each website in conjunction with the ICT coordinator and link ICT Governor and ensure that content is accurate and appropriate.

iv. Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website 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 Website.

v. 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 may be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

vi. Managing filtering

- The school will work with their nominated ICT support provider 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 (ICT) Coordinator. The Internet Service Provider provides a filtering service and the Headteacher is notified of any blocked sites for further investigation.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

vii. Managing videoconferencing

- School uses Zoom parents' evenings when required.
- Invitations are sent to parents/carers securely via SchoolSpider for online Parents Evenings.
- Teachers use the waiting room function and ask that people use their real name so they are easily identifiable. Anyone we don't recognise is not admitted and cannot join the call.
- Parents are asked to supervise children at all times when engaging with a live Zoom meeting.

viii. Managing emerging technologies

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

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Pupils are not allowed to bring mobile phones into school.
- Staff will not use personal equipment or non school personal electronic accounts when contacting students. The school phone will be used where contact with pupils is required.

ix. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018. Please refer to CDAT Data Policies.

Policy Decisions

i. Authorising Internet access

- All staff must read and sign the CDAT Acceptable Use Policy – Workforce before using any school ICT resource.
- All pupils and their parents/carers must read and agree to the CDAT Acceptable Use Policy - Pupils. This will be issued to parents/carers with the school's Home School Agreement and Parents will be asked to sign to give permission for their child to have access to the internet and ICT systems in school
- The school will keep a central record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. It is the Headteacher's responsibility to ensure that the record is kept up to date so that it can be easily referred to.
- Within the Primary school access to the Internet will be supervised. Lower down the school access will be to specific, approved online materials.

ii. 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 not possible to guarantee that unsuitable material will never appear on a school computer. Neither the School nor the local authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

iii. Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/ Headteacher
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and referred to the Headteacher as Designated Safeguarding Person or the School. Pupils and parents will be informed of the complaints procedure and the School Complaints Policy will be followed.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

iv. Communications Policy

Introducing the E-Safety Policy to pupils

- E-safety rules will be posted in all networked rooms 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 have access to the School E-Safety Policy via the School Website.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

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

E-Safety Policy	
Review Frequency:	Annual
Reviewed and approved by:	Local Governance Committee
Date reviewed/approved:	9th December 2024
Date of next review:	9th December 2025