- Everyday Excellence
- Authentic Care
- Independence
- Opportunity

# The Quinta Primary School

Online Safety Policy

| | |
|---|---|
| Approved by: | SLT - June 2021 |
| Last reviewed on: | 17.06.2021 by W.Sharpe, PHSCE team & Computing team |
| Next review due by: | June 2023 |

| Changes since last review | |
|---|---|
| renamed policy | online safety changed to Online Safety |

Our online safety Policy has been written by the school, building on the Cheshire eSafety Policy and government guidance. It has been agreed by senior management and approved by governors.

## 1.What is Online Safety?

Online safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, 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.

The school's online safety policy will also run in conjunction with the Behaviour, anti-Bullying and Acceptable Use policies.

## 2.Rationale

The Internet is now considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning. This online safety policy considers the use of both the fixed and mobile internet, PCs, laptops, tablets, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players. It will be revised to incorporate new and 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 purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use.

The school will ensure that all members of the school community are aware of the online safety policy and the implications for the individual. online safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

## 3.Guidance

End to End online safety

online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband Network including the effective management of Website filtering.
- National Education Network standards and specifications.

## 4.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.
- Where Internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the school.

## 5.Internet use will enhance learning

The school Internet access is designed for pupils and family use and includes 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
- The children access the internet to make use of the school's learning platform, collaborative work e.g. shared documents whilst learning about safe and secure use of the internet, messaging, forums and personal web pages. These will be closely monitored by staff and the teaching of safe practice online will feature in every online lesson.

## 6.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.

## 7.Managing Internet Access

**Information system security**

- School ICT systems and security will be reviewed regularly. *(Please refer to the Appendix 1)*
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.

## 8.E-mail and Messaging

Pupils must immediately tell a teacher if they receive offensive messages which will also become alerts on the staff login area of the website.

- Pupils must not reveal personal details of themselves or others in any 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.
- If staff use email as a means of communicating with other agencies or colleagues in other schools, this should be done so through their school's email account.

## 9.Published content and the school website

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

## 10.Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified in the website or public content areas.

- Pupils' full names will not be used anywhere on the Web site or Blog 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 in the child's planner and signed at the start of the year
- Pupil's work can only be published with the permission of the pupil and parents on Seesaw and class blogs

## 11.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.
- Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social networking site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils and they should refer the Staff Acceptable Use Policy.

## 12.Managing filtering

The school's internet is filtered through a proxy server and a firewall managed by EXA networks. The school also employs a fortnightly technician to manage the service and technical support, ensuring the filtering is constantly reviewed and up to date.

- If staff or pupils discover an unsuitable site, it must be reported to the computing team who should be known to all members of the school community and then the issue should be referred to the LA ICT helpdesk.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## 13.Managing video conferencing - In the event that video conferencing is used:

- IP video conferencing should use the educational broadband 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 video conference call.
- Video conferencing will be appropriately supervised for the pupils' age.

## 14.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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will not use personal equipment or non school personal electronic accounts when contacting students or parents. They will be issued with a school phone where contact with pupils is required. For further guidance, staff should refer to their Acceptable Use Policy.

## 15.Protecting personal data

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

## 16.Policy Decisions

**Authorising Internet access**

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource.

- All students and their parents must read and agree to the 'Students' Safety Rules in the Pupils' Acceptable Use Policy'.
- Parents will be asked to agree to and return a consent form in their child's planner with respect to the 'Students' Safety Rules' in the Pupils' Acceptable Use Policy.
- The school will keep a record of all staff, pupils and governors who are granted access to the Learning Platform and of any children who do not have parental permission to use the internet. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

- Within the Primary school access to the Internet will be supervised. Lower down the school staff will direct learning to specific, approved on-line materials.

## 17.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 online safety policy is adequate and that its implementation is effective.

## 18.Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and in line with the school's complaint policy.
- 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.

## 19. Introducing the online safety policy to pupils

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

Pupils will be taught to follow the 10 rules for staying safe on-line as outlined below:

1. *Don't give out personal info*
2. *Tell if you find something that is not right*
3. *Don't agree to meet people*
4. *Never send your picture*
5. *If some one says something mean online tell a grown up*
6. *Don't do things online you know are wrong*
7. *Check before you download anything*
8. *Don't give out your password*
9. *Set up rules for going on line*
10. *Show your Parents and Carers how you use the internet. SHARE*

## 20. Staff and the online safety policy

- All staff will be given the School online 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 is essential.
- All staff and governors with access to ICT equipment or learning platform will be asked to sign the Acceptable Use Policy

## 21. Enlisting parents' support

- Parents' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school Web site.
- Parents will be asked to talk to their children about the school's Acceptable Use Policy and staying safe on-line before signing and returning it to school

**Appendix 1**

Considerations around access to data from, into and within the school are as follows

Where a school is part of the Connected Cheshire network then external security to and from the school is managed by firewalls administered by Connected Cheshire.

Additional protection is provided by filtering services for web traffic and external email traffic which are managed by Connected Cheshire. Where a school has a concern that filtering is not blocking inappropriate websites it is their responsibility to contact Connected Cheshire Help Desk to report the website. Secondary Schools can manage their filtering over and beyond the service provided by Connected Cheshire.

Where a school buys into a third party ISP service then generally the responsibility to provide firewalls and filtering services is with the schools.

Schools should take responsibility for deciding who is allowed access to data within and external to the school through the use of an authentication policy (user identification and passwords need to be issued and managed)

It is the school's responsibility to ensure that the security of any wireless networks is set to block unauthorised access. Where possible the school should seek to upgrade systems to meet the County recommended standard which is available from the ICT section on the Cheshire Learning Portal.

It is good practice to set screen savers to engage after a maximum of 20 minutes which **require the user to log back** in when deactivated. This helps maintain security of systems by minimising the risk of computers being left logged on for extended periods of time and enabling user accounts to be abused by unauthorised users.

Virus protection should be installed on every computer and should be set to update automatically at least every week if not daily.

**Guidance on internet use - Possible teaching and learning activities**

| Activities | Key online safety issues |
|---|---|
| Creating web directories to provide easy access to suitable websites. | Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be directed to specific, approved on-line materials. |
| Using search engines to access information from a range of websites. | Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. |
| Exchanging information with other pupils and asking questions of experts via e-mail. | Pupils should only use approved e-mail accounts.<br>Pupils should never give out personal information.<br>Consider using systems that provide online moderation e.g. The Learning Platform. |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication.<br>Pupils' full names and other personal information should be omitted. |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought.<br>Photographs should not enable individual pupils to be identified.<br>File names should not refer to the pupil by name. |
| Communicating ideas within chat rooms or online forums. | Only chat rooms contained with the schools Learning Platform and linked to educational use and that are moderated should be used.<br>Access to other social networking sites should be blocked.<br>Pupils should never give out personal information. |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised.<br>Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. |

## Guidance in response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any online safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to online safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Coordinator, the online safety Officer or the Police Liaison Officer.

***What does electronic communication include?***

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

***What are the risks?***

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breach

***How do we respond?***

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Child Protection Unit and Designated staff member should be consulted.

As previously stated schools should ensure that relevant policies (Acceptable Use Policy, Behaviour Policy, Bullying Policy, Discipline Policy) are referenced and are considered when dealing with the issues identified.