

# Queensgate Primary School

## E-safety Policy



<b>Date of Policy</b>	<b>Date approved by Governing Body</b>
<b>2016</b>	<b>2016</b>

<b>REVIEW SCHEDULE</b>			
<b>Date of next Review</b>	<b>Date reviewed by Governing Body</b>	<b>Change previous document (Y/N)</b>	<b>Date circulated (if changes)</b>
<b>Spring 2019</b>	<b>Spring 2019</b>	<b>Y</b>	<b>Spring 2019</b>
<b>Spring 2021</b>		<b>N</b>	
<b>Spring 2023</b>		<b>N</b>	

## **Introduction**

At Queensgate we recognise that ICT and the use of the Internet plays an important role in children's learning. It is important that the children in our school see both the benefits and the risks of using new technologies. Our E- Safety policy explains the need for providing safeguards and awareness for users to enable them to control their online experience.

The school's E-safety policy also operates in conjunction with other policies including those for Behaviour (incorporating Anti-Bullying, Curriculum and teaching and learning, and Data Protection.)

## **Teaching and learning**

### **Why Internet use is important**

- The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to 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 is designed expressly for pupil use and uses central LA filtering services to ensure content that is accessed is appropriate to the age of pupils.
- At Queensgate, pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. This will be completed in both Computing and PSHE lessons.
- During lessons, our children 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**

- At school, we will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Through our Computing, and PSHE lessons, our pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

## **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 Stockport local authority and developed with our ICT technician.

### **E-mail**

- Pupils do not have access to any e-mail accounts on school systems.
- Through our specific lessons, children at Queensgate are taught not to reveal personal details of themselves or others in e-mail communication, to open messages from unknown parties, or to arrange to meet anyone without specific permission.

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

- The contact details on our school website are the school address, e-mail and telephone number. Staff or pupils' personal information is **not** published.
- The head teacher takes overall editorial responsibility of the website and ensures that content is accurate and appropriate.

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

- Pupils' full names will not be used anywhere on the website, blog or twitter, particularly in association with photographs.
- Written permission will be sought annually from parents or carers before photographs of pupils are published on the school website/twitter.
- Pupil's work can only be published with the permission of the pupil and parents.

### **Social networking and personal publishing**

- The school and LA block access to social networking sites with the exception of twitter.
- Pupils are routinely advised never to give out personal details of any kind which may identify them or their location, or to accept 'friend requests' or respond to other messages from unknown parties, and to report these where appropriate.
- Pupils are made aware of the dangers of social network spaces and how to minimise the risk
- Parents are made aware of the dangers of social network spaces and how to promote responsible use at home.

### **Managing filtering**

- 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 Computing Lead and logged on CPOMS.
- 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 are not permitted for use by pupils in school.
- Staff should not use their mobile phones in the presence of pupils (see Safeguarding Policy for further details)
- Pupils and their parents accept full responsibility for any personal 'devices' which they choose to bring into school to assist them with their work.
- 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.

## Policy Decisions

### Authorising Internet access

- Annually, all staff must read and sign the “ **Computing and ICT Code of Conduct**” before using any school ICT resource.
- 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 member of staff may leave or a pupil’s access be withdrawn.
- Children and parents must sign the **PUPIL & PARENTS/CARERS E-SAFETY ACCEPTABLE USE AGREEMENT** before using any school ICT resource.

### 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 Stockport LA can accept liability for the material accessed, or any consequences of Internet access.
- 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 safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.

### Community use of the Internet

- The school will liaise with local and national 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 networked rooms and discussed with the pupils at the start of each year.
- Pupils will be reminded of the E-safety rules at the beginning of each half term and regularly referred to throughout the year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be educated in safe internet use in the home.
- The school will inform parents about E-safety so they can use the internet safely at home.
- Parents will have the opportunity to discuss any concerns with a member of staff

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

- All staff will be given the School e-Safety Policy and its importance explained. It will be referred to in the Staff Handbook and will therefore be discussed during induction of any new staff and each September (INSET).
- 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, at e-Safety events and on the school website.

**QUEENSGATE PRIMARY SCHOOL**

**PUPIL & PARENTS/CARERS E-SAFETY  
ACCEPTABLE USE AGREEMENT**

***All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.***

***Pupil:***

***Class:***

**Pupil's Agreement**

- I have read and I understand the school e-Safety Rules.
- I will use the computer, iPads, network, digital cameras, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

***Signed:***

***Date:***

**Parent's Consent for Web Publication of Work and Photographs**

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

**Parent's Consent for Internet Access**

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

**Parents should:**

- discuss e-safety issues with their children
- ensure their children access age appropriate websites and social media
- ensure their children communicate respectfully and maintain responsible standards when communicating on the internet and social media
- inform the school if they think there is an e-safety issue related to the school
- maintain their own responsible standards and communicate respectfully about Queensgate Primary School when communicating on social media and the internet

***Signed:***

***Date:***

***Please print name:***

## Queensgate Primary School Staff Code of Conduct for Computing & ICT

***To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-safety Policy and Computing Policy for further information and clarification.***

- I understand that it is a criminal offence to use a school Computing & ICT system for a purpose not permitted by its owner.
- I appreciate that Computing & ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that Computing & ICT use may also include personal devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security, use only the individual login that I have been given and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely through encrypted memory devices.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Online Safety Coordinator, the Designated Safeguarding Lead or the Headteacher.
- I understand that electronic communications outside school with pupils and parents including email and social networking are not compatible with my professional role and that communication about school issues should not be encouraged and that such communications could contravene the terms and conditions of my employment.
- I understand that any photographs taken of pupils (for the purposes of uploading to the school's social media sites or otherwise) should be taken using the school's equipment. Where school's equipment is not available and personal equipment is used (such as a mobile phone) images should be deleted as soon as possible and such devices should not be taken off the school's premises until such images have been deleted.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

**I have read, understand and accept the staff Code of Conduct for Computing & ICT.**

**Name:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**Signed:** \_\_\_\_\_