Online E-Safety Policy

Person responsible: Chris Wilson
Date adopted/reviewed: June 2019, May 2020, May 2021
Date of next review: May 2022
Governor's signature: D Bishop

Aims

This policy and related documents apply at all times to the use of computing devices including but not limited to laptop or desktop computers, tablets and mobile phones which are owned and supplied by the school and to personal devices owned by adults or young people while on the school premises. The policy also encompasses; electronic communications, collaboration tools and personal publishing and operates alongside the Acceptable Internet Use Agreements.

Procedure

Publicising Online Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at: http://www.queensburysch.com
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant online safety information in all areas where computers are used
- Provide online safety information for parents and through the school newsletter
- Educate the pupils in staying safe online

Roles and Responsibilities

The Head Teacher and Governors have ultimate responsibility for establishing safe practice and managing online safety issues at our school. The role of ESafety Co-ordinator has been allocated to the Pastoral Manager supported by the ICT Manager. They are the central point of contact for all online safety issues and will be responsible for day-to-day management.

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the E-Safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network
- Understand that the use of school owned devices are monitored when they are attached and not attached to the school network

- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Physical Environment/Security

The school endeavours to provide a safe environment for the whole community, we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Link2ICT. All staff and students understand that if an inappropriate site is discovered it must be reported to the E-Safety Co-ordinator who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the online safety log for audit purposes.
- Requests for changes to the filtering will be directed to the ICT Manager in the first instance who will forward these on to Link2ICT or liaise with the Head Teacher as appropriate.
- The school uses Net DNA monitoring on school owned equipment to ensure compliance with the Acceptable Internet Use Policies and is checked on a regular basis by designated members of staff
- All staff and students are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's.

Mobile/emerging technologies

- Teaching staff at the school are provided with a laptop/iPad for educational use. All staff understand that the Acceptable Internet Use Policies apply to this equipment at all times.
- School mobile phones are issued to staff that may need to contacted parents
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should not use mobile phones during teaching time and usage must be in line with school policy.
- Pupils understand that they must hand their mobile phones into the school office during school hours.
- The Educations and Inspections Act 2006 grants the Head Teacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head Teacher will exercise this right at her discretion
- Pictures/videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-mail

- A school e-mail system is provided and is governed by Microsoft Office 365
- All staff are given a school e-mail address and understand that this must be used for all professional communication
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Staff are allowed to access personal e-mail accounts on the school system outside directed time, they also understand that these messages will be scanned by the monitoring software

Published content

- The Head Teacher takes responsibility for content published to the school web site but delegated members of staff have editorial responsibility.
- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office/generic e-mail addresses
- The school does not publish any contact details for the pupils

Digital Media

We respect the privacy of the school community and will obtain written permission from parents or carers before any images or video are published or distributed outside the school.

- Photographs will be published in line with national guidance and not identify any individual pupil
- Students' full names will not be published outside the school environment

Social Networking and online communication

The school is constantly reviewing the use of social networking sites and online communication and currently allows limited access for designation staff to sites such as Twitter and Facebook for communication about school events only.

- Staff oversee the safe use of electronic media and take action immediately if they are concerned about bullying or risky behaviours
- Pupils are not permitted to use social media in school
- Pupils have access to school email accounts which can only communicate internally and are taught how to communicate responsibly, safely and respectfully.
- Guidance is provided to the school community on how to use these sites safely and appropriately. This includes:

○ not publishing personal information ○ not publishing information relating to the school community ○ how to set appropriate privacy settings ○ how to report issues or inappropriate content

- Unmoderated chat sites present an unacceptable level of risk and all known sites are blocked in school, any sites that are not blocked must be reported to the E-Safety Officer. Pupils are given age appropriate advice and guidance around the use of such sites.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information
- Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Internet Use Polices before any activity
- Acceptable use Agreements must be accepted before accessing school equipment.

Safeguarding

Ensuring pupils and staff are protected and feel safe, that online safety issues are dealt with inline and as part of whole school safeguarding procedures

- Pupils will be educated about online risks including online bullying and sexting (where school deems age appropriate) and who they should talk to if they feel unsafe
- Strategy and procedures supported by whole staff training are in place ensuring staff understand the risks posed by adults or learners who use technology, including the internet, to bully, groom, radicalise or abuse pupils, and how to take action in any event that raises concern

Data Security/Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998. Data is stored on the school systems and transferred in accordance with the Local Authority Data Security/SIRO Guidelines

Wider Community

Non-school; based users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Safeguarding Policy.

- Any suspected illegal activity will be reported directly to the police.
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head Teacher
- Breaches of this policy by staff will be investigated by the Head Teacher. Action will be taken under Schools Disciplinary Policy
- Student policy breaches relating to bullying, drugs and abuse must be reported to the E-Safety coordinator and action taken in line with school anti-bullying Safeguarding. There may be occasions when the police must be involved.
- The Educations and Inspections Act 2006 grants the Head Teacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

Acceptable Internet Usage

The computer systems are owned by the school and made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an AUP drawn up to protect all parties -the pupils, the staff and the school. The school reserves the right to examine or delete any internet data that may be held on its computer systems or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- Posting anonymous messages and forwarding chain/spam or viral emails is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- All Internet use should be appropriate to staff professional activity or to children's education.

- Personal devices (Phones/Tablets/Laptops) must not be connected to the school network.
- You must not download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. You will not try to use any programs or software that might allow you to bypass the filtering / security systems in place to prevent access to such materials.
- You will not access, save, download or print any materials that promote political or religious Extremism/Radicalisation.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The use of public chat rooms and personal social media is not allowed.
- Staff must not 'befriend' parents or students on social networking sites.
- Mobile phones are to be switched off during lesson time, Texts must only be sent from the classroom or staffroom outside of lesson time.
- Staff are allowed to check their personal email on a limited basis as long as it does not interfere with their job responsibilities and does not take place during teaching or supervision time. Members of staff are reminded that they should not deliberately seek out inappropriate/offensive materials on the Internet and that they are subject to the LEA's recommended disciplinary procedures should they do so.