The Quest School

Online Safety and Acceptable Use Policy

Date	Review Date	BoM	Co author
Sept 20	Sept 21	Peter Mepsted	Jo Allcorn / Ellie Drake

This policy relates to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2003
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012
- Data Protection Act 2018

The following documentation is also related to this policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, School Principals, School Staff, Governing Bodies and Proprietors of Independent Schools (DfE)
- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE) (2018)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children (2015)
- Searching, screening and confiscation (DfE)
- Preventing and tackling bullying (DfE)
- Protecting children from radicalisation (DfE).

There are other school policies which are to be considered in addition to the document, including:

- Data Protection Policy
- GDPR Operation Guidance
- Code of Conduct
- Policy for Safeguarding

We have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

Online safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the school community have an entitlement to safe Internet access at all times.

We wish to work closely with pupils to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

Aims

- To provide pupils with quality Internet access as part of their learning experience across all curricular areas.
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To evaluate Internet information and to take care of their own safety and security.
- To raise educational standards and promote pupil achievement.
- To work with other schools and the local authority to share good practice in order to improve this policy.

Anti Radicalisation and Extremism

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremists groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. School personnel must be aware of the risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school personnel are able to identify those who

may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment, we work hard to build pupils' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views.

Responsibility of the Policy and Procedure

Role of the Board of Management

The Board of Management has:

- appointed a member of staff to be responsible for online safety;
- delegated powers and responsibilities to the School Principal to ensure all school staff and stakeholders are aware of and comply with this policy;
- responsibility for ensuring that the school complies with all equalities legislation;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- make effective use of relevant research and information to improve this policy;
- responsibility for ensuring policies are made available to parents;
- relevant members of the Board of Management to undertake training in order to understand online safety issues and procedures;
- responsibility for the effective implementation, monitoring and evaluation of this policy.

Role of DSL and Head of Operations

- To oversee the implicational processes of this policy.

Role of the School Principal

The School Principal will:

- ensure the online safety and online safety of all members of the school community;
- ensure all school personnel are aware of and comply with this policy;
- work closely with the Board of Management and the coordinator to create a safe ICT learning environment by having in place:
    - an effective range of technological tools
    - clear roles and responsibilities
    - safe procedures
    - a comprehensive policy for pupils, staff and parents
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- embed online safety in the curriculum

- provide leadership and vision in respect of equality;
- make effective use of relevant research and information to improve this policy;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy by:

    - monitoring learning and teaching through observing lessons
    - monitoring planning and assessment
    - speaking with pupils, school staff, parents and trustees

Role of the Online Safety Coordinator

The coordinator will:

- be responsible for the day to day online safety issues;
- have completed a suitable level of training under an approved board
- undertake periodic online safety audits three times a year in order to establish compliance.
- ensure that all Internet users are kept up to date with new guidance and procedures;
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- undertake risk assessments in order to reduce Internet misuse;
- maintains a log of all online safety incidents which will be reviewed regularly. The Online safety coordinator will report serious breaches to the Board of Management/school principal. A serious breach will be determined by the Online safety coordinator based on experience
- reports all online safety incidents to the School Principal;
- ensure online safety is embedded in the curriculum
- lead the development of this policy throughout the school;
- work closely with the School Principal
- make effective use of relevant research and information to improve this policy;
- provide guidance and support to all staff;
- ensure all staff have read and signed this policy on induction and when it is updated;
- keep up to date with new developments and resources;

Role of School Staff

School staff will:

- Comply with all aspects of this policy
- Undertake appropriate training;
- As far as possible, verify the source of any web materials before using them with pupils; check domain type or organistaion if in doubt.
- Be responsible for promoting and supporting safe behaviours with pupils;
- Promote online safety procedures such as showing pupils how to deal with inappropriate material;
- Report any unsuitable website or material to the online safety Coordinator;
- Will ensure that the use of Internet derived materials complies with copyright law;
- Ensure online safety is embedded in the curriculum and other school activities;

- Be aware of other linked policies;
- Maintain high standards of ethics and behaviour within and outside school and not to undermine fundamental British values;
- Implement the school's equalities policy and schemes;
- Report and deal with all incidents of discrimination;
- Attend appropriate training sessions on equality;
- Report any concerns they have on any aspect of the school community
- All use of Quest School's resources must be for professional and curriculum purposes only. Inappropriate use of school equipment is 'unauthorised' and any persons found to have contravened these rules, risks disciplinary measures.
- Staff will not download or install unauthorised software onto either networked or laptop computers.
- Staff will not, under any circumstances view, upload or download any material that is likely to be unsuitable for children.
- Staff must not use any equipment provided by the school or use any personal equipment to bully or harass others.
- Staff should not use their own personal memory sticks on any school computers. School memory sticks should only be used in exceptional circumstances.
- Staff password and login details must not be divulged to pupils or any other persons not in the employ of Quest School except on the authority of the School Principal. Any breach of this will be considered as gross misconduct.
- When leaving a work station, staff must ensure they have logged off the network, or have their computer password protected which locks on shutdown of the laptop lid to prevent unathorised access to the server by either pupils or other staff who have restricted access to the server. The Control/alt/delete function can also be used. This includes communal equipment such as the Clever touch screens in the group lesson rooms. The only exceptions to this is in an emergency situation where the emergency has a potential higher risk of delayed responding to than not logging off the network or when there are other people in the room with the same server access who can ensure an unauthorised person will not use their computer
- All Quest laptops and desktop computers must be password protected enabling only authorised personnel to use that machine
- Staff must ensure that when they have used a school camera or photograph taking instrument that photos with the pupils in or sensitive information are uploaded onto the server and wiped from the device before the end of a term. Photos without the pupils in them may be left on the device if they are needed for programme resources.
- At the end of the school academic year, all information on all devices will be wiped.
- Quest laptops and computers should not have information or work saved to them that contains sensitive information about staff or pupils. Senior members of staff may save presentations or training material to the laptop directly if they are training or presenting offsite. However, their laptop must remain with them whilst they are offsite at all times.
- Staff must not attempt to destroy or corrupt others' data or to access areas of the server where they are not permitted
- Staff must be aware that all network activity and online (when using the Quest wifi) are monitored, including any personal and private communications
- Quest emails are the property of The Quest School and are continually monitored. This includes all email content.
- The Quest email account must be logged off on any shared computer.

- Personal use of mobile phone for voice or text communication within school is strictly forbidden whilst supervising pupils.
- Personal mobile phone use is also forbidden whilst supervising pupils off-site. School mobiles only should be used. The only exception for this is the event of an emergency evacuation such as a flood where communication between staff member will be vital.
- Personal use of the internet and email system must only be used on authorised breaks and to be restricted to staff only areas of the school. Personal use of the internet or material found should under no circumstance be shared with any pupils. Personal use must not occur on Quest laptops or computers which the pupils access.
- Only Quest related work should be saved on the Quest server
- Staff must not at any time give their personal details such as phone numbers to pupils, nor should they accept such details from pupils
- Staff must not accept pupils or parents/carers as 'friends' on social media.
- Editorial responsibility of the school Web site rests with the HR Manager, who will amend content by agreement with the BoM.
- **Tapestry:** sharing information with parents via Tapestry is done so in accordance with internal guidance

Guest Access to the School WIFI

- Quest Guest will operate under a different VLAN to the other school access. This will have less filters than other routes.
- The password for this will be kept with three designated members of the school office staff and must not be disclosed to any other staff or visitor to the school. This password will be changed frequently
- All access on Quest Guest will be monitored.
- Quest staff must only access the wifi through the BYOD WIFI on their own devices or the usual school WIFI on school laptops.

Remote working:

- Remote working should be inline with GDPR Operational Guidance document.
- Remote access to school emails and systems on your personal device (e.g. smart phone or tablet) is permitted only with consent from the Data Protection Officer.
- You must ensure that all data is cleared off the device if you cease to use the device or cease to be employed at the Quest School.
- If your device is lost or stolen please inform the Data Protection Officer as soon as practically possible as this may be a security concern.
- When working remotely on school laptops, staff must ensure the laptop is only accessible to themselves as an employee of the Quest School
- All staff removing laptops / tablets from site (for whatever reason) will take all reasonable precautions to safeguard the equipment from loss or damage
- Any school device must be password protected and never left unattended whilst unlocked. If the workstation is left, staff must log off of the network or lock the computer by pressing control/Alt/Delete or by closing the laptop lid
- For non-remote access, the documents that contains sensitive information about staff or pupils (password protected) must be emailed to yourself rather than storing them on a

desktop to transport. Once the work has been completed, it must be emailed back to yourself and the document deleted off the desktop.

- Staff who bring their own device to work on must only do so for resource planning purposes. No staff member will save anything that can identify a pupil (name, personal details or photo) to their own device.
- For those with permission to remotely access the schools' network, Smoothwall must be used to provide direct access. Other methods of access to the schools server are not permitted.

Video Conferencing:

- Teams is the preferred method for online meeting and communication. Zoom can be used in an instance where Teams is not appropriate, but only with the consent of the DPO.

Role of Pupils

Pupils will be taught to:

- Be critically aware of the materials they read;
- Validate information before accepting its accuracy;
- Acknowledge the source of information used;
- Use the Internet for research;
- Respect copyright when using Internet material in their own work;
- Report any offensive e-mail;
- Report any unsuitable website or material to the online safety Coordinator;
- Know and understand the school policy on the taking and use of photographic image and cyber bullying;
- Pupils will not download or install unauthorised software onto either networked or laptop computers.
- Pupils should not use their own personal memory sticks on any school computers. School memory sticks should only be used in exceptional circumstances.
- Personal use of mobile phone for voice or text communication during school hours is strictly forbidden except with authorisation from a senior member of staff.
- Personal use of the internet, social media sites and email system is forbidden during school hours, unless as part of a specific lesson and supervised by staff.
- Pupils must be aware that when unacceptable use is suspected, additional monitoring procedures might come into force such as checking and/or confiscating personal devices.
- Pupils must be aware that all network activity and online (when using the Quest wifi) are monitored, including any personal and private communications
- Pupils must not give the password to their section on the server to any person not employed by Quest.
- Pupils must not access, view or amend other pupils' work on the server and pupils will be made aware there will be a consequence to this behaviour if it was to occur.

Role of Parents / Carers

Parents/carers will:

- be aware of this policy;
- be asked to support the online safety policy
- make their children aware of the online safety policy;
- be encouraged to take an active role in the life of the school by attending:
    - parents and open evenings
    - parent-teacher consultations
    - Online training via school website

Internet Use

The school Internet access will:

- Be designed for pupil use;
- Include school filtering configuration which is designed to protect pupils;
- Provide filtering which is reviewed regularly and improved if necessary;
- Include filtering appropriate to the age of pupils;
- Have virus protection installed which will be updated regularly;
- Be reviewed and improved
- Staff will provide appropriate supervision at all times for pupils using the internet.

Pupil Access

Pupils will not be allowed to access:

- Social networking sites except those that are part of an educational network or approved Learning Platform.
- Newsgroups unless an identified need has been approved.

Staff Access

- Staff will have the ability to access the internet on the school laptops for work purposes. Staff should only access appropriate and trusted websites.
- Staff must report any unsuitable website or material to the Online Safety Coordinator.

E-mail

Pupil Usage

Pupils must:

- Only use approved e-mail accounts;

- Report receiving any offensive e-mails;
- Not divulge their or others personal details;
- Not arrange to meet anyone via the e-mail;
- Seek authorisation to send a formal e-mail to an external organisation
- Not take part in sending chain letters

Staff Usage

- Staff at Quest will be given an email account. Tutors will have the ability to send and receive email internally only, other staff will have the functionality to send and receive external and internal emails.
- Staff must report and suspicious emails or material to the Online Safety Coordinator or Data Protection Officer.
- All staff should consider whether an email (by incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder on the network drive or printed and stored securely.

School Website

Contact details on the website will be:

- the school address
- e-mail address
- telephone number

The school website will not publish:

- staff or pupils contact details;
- the pictures of children without the written consent of the parent/carer;
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer

Access to change the content on the Quest website is limited to those individuals who have been granted access rights by the BoM. Persons granted access can be seen in Appendix 1.

Social Media

Quest uses Facebook and Twitter social media platforms as a marketing and communication tool.

Access to Quest social media accounts is limited to persons given specific access. Details of these individuals can be found in Appendix 1. Access rights are granted by the BoM and only those staff members who have been given access rights are authorised to post content.

Inappropriate Material

Any inappropriate websites or material found by pupils or school personnel will be reported to the online safety Coordinator who in turn will report to the Internet Service Provider.

Internet System Security

- New programs will be installed onto the network or stand-alone machines by authorised school technicians only.
- Personal memory sticks, CDs and other data recording devices may not be used in school.
- Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence.

- The School uses **Smoothwall** for internet security which is:
- Smoothwall Filter categorises web content in real-time, without dependence on unreliable and outdated URL blocklists. It has a reporting suite, social media controls and BYOD functionality. Smoothwall Filter enables the school to review and control what students see online
- The Firewall is a unified threat management solution that protects the network and users against web and non-web borne threats. It has Layer 7 application control with perimeter firewall and stateful packet inspection.
- Smoothwall Firewall is able to identify over 100 different kinds of traffic - even when the traffic doesn't want to be identified
- Smoothwall Monitor is a real-time, digital monitoring solution that flags incidents as they happen. Monitoring both keystrokes and screen views, safeguarding staff are informed, through a variety of means, when users try to view or type harmful content.

Tablets and Handheld Devices System Security

- All of the school's Tablets and Handheld devices are managed by Lightspeed MDM Systems which is a system built for schools. This allows the device to be controlled remotely by the ICT co-ordinator and prevents access to the settings by staff and pupils thus preventing any unathorised changes to the device.
- All apps that allow external file sharing are blocked and cannot be accessed.
- All devices have the same passcode. Pupils must never be told the passcode.
- The devices must be connected to the Quest wifi at all times to ensure the internet is filtered.

Complaints of Internet Misuse

- The School Principal will deal with all complaints of Internet misuse by school personnel or pupils.
- Parents will be informed if their child has misused the Internet.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- the School Handbook/Prospectus
- the school website
- the Staff Handbook
- meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops

- school events
- meetings with school staff

Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

Monitoring the Effectiveness of the Policy

The practical application of this policy will be reviewed on our regular cycle or when the need arises by the coordinator, or School Principal.

Appendix 1

Social Media and Website access rights

	Facebook	Twitter	Quest News	Quest Website
Authorised users	Jo Allcorn Ellie Drake Julie Yeomans	Jo Allcorn Peter Mepsted	Jo Allcorn Julie Yeomans	Ellie Drake Ross Hardy (Website and Media Consultant)