QUEEN ELIZABETH’S SCHOOL (WIMBORNE MINSTER)

E - Safety Policy

Review:

Title of Policy	E – Safety Policy
Review Cycle	Annually
Policy prepared by	Gavin Rusling, Assistant Headteacher & DS Lead
Committee responsible	Community and Environment
Date of review by committee	13th September 2018
Date of approval or submission to FGB	25th September 2018
Next Review	Under Review

1. Introduction and Purpose

The Education and Inspections Act 2006 and the White Paper of 2016 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are both on and off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place both on and outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

2. Scope

This policy applies to all members of Queen Elizabeth's School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

3. Legal Requirements.

- Education and Inspections Act 2006 and the White Paper of 2016
- Education Act 2011

4. Principles, Responsibilities and Procedures

This e-safety policy has been developed by a working group / committee made up of:

- Headteacher /Senior Leaders
- E-Safety Champion
- Staff – including Teachers, Support Staff, Technical staff
- Governors

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school

4.1 Governors

Governors are responsible for the approval of the E-Safety Policy and have designated the Community and Ethos Committee as having the lead for reviewing the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor and they are also responsible for Child Protection and Safeguarding. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Champion
- reporting to relevant Governors committee meeting and Full Governing Body.

4.2 Headteacher / Principal and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Champion.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Champion and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. (The school / academy will need to describe this and may wish to involve the Local Authority / other responsible body in this process).

4.3 E-Safety Champion

The e-safety champion for Queen Elizabeth's School is Gavin Rusling

- leads the E-Safety Group
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- monitors reports of e-safety incidents and supervises the log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends C & E committee of Governors
- reports regularly to Senior Leadership Team

4.4 Network Manager / Technical Staff:

IT Systems Manager reporting to the Chief Operating Officer is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- That the academy meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

4.5 Teaching and Support Staff

Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- When working away from a logged on workstation – it is locked
- Staff using mobile devices to check emails or access the network must have a pin code enabled on the device.

- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Champion for investigation
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.6 Designated Safeguarding Lead (DSL)

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

4.7 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school

4.8 Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. (A Community Users Acceptable Use Agreement Template can be obtained from the E – Safety champion.

5.0 Educational Aims

5.1 Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of ICT and PHSE and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet

searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

5.2 Parents /Carers

The ever changing nature of e-safety and therefore the different risks and issues that come about, make it a difficult task for parents/carers to keep abreast of, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk -www.saferinternet.org.uk/- http://www.childnet.com/parents-and-carers-www.ceop.police.uk

6. Links and References

- Bullying Policy
- Behaviour Policy
- Confidentiality Policy
- Social Networking Policy
- BYOD Policy
- Data Protection

7. Review

This policy will be reviewed annually by the SLT Sponsor, Headteacher and Committee. Amendments will be recommended to the Governing Body for adoption or approval as appropriate.