

**E-Safety Policy**

**To be read in conjunction with the password policy, AUPs, Behaviour and Discipline Policy and Anti-Bullying Policy**

5

**Schedule for Development / Monitoring / Review**

|  |  |
| --- | --- |
| This e-Safety Policy was initially approved by the Governors Committee on: | *March 2015* |
| This e-Safety Policy was last review by the Governors Committee in | *May 2017* |
| The implementation of this e-Safety Policy will be monitored by the: | *ICT Co-Ordinators and the Curriculum & e-Safety Committee* |
| Monitoring will take place at regular intervals: | *Annually* |
| The Governors Committee will receive a report on the implementation of the e-Safety Policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: | *Once a year* |
| The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *July 2021* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Police, LA Safeguarding Team* |

The school will monitor the impact of the policy using:

* Logs of reported incidents on CPOMs
* Monitoring logs of internet activity (including sites visited)
* Internal monitoring data for network activity
* Surveys / questionnaires of:

- students / pupils

- staff

**Scope of the Policy**

6

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are 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 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.

**Roles and Responsibilities**

7

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

**Governors:**

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum and e-Safety Committee who receive regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of e-Safety Governor. The role of the e-Safety Governor will include:

* regular meetings with the e-Safety Co-ordinator / Officer
* regular monitoring of e-Safety incident logs
* regular monitoring of filtering / change control logs

**Head teacher and Senior Leaders:**

* The Head teacher 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 Co-ordinator.
* The Head teacher and (at least) another member of the Senior Management 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 Head teacher and Senior Leaders are responsible for ensuring that the e-Safety Coordinator 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 Head teacher 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 Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator.

**E-Safety Coordinator:**

* leads the e-safety committee
* 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 as appropriate
* liaises with school technical staff
* receives reports of e-safety incidents and creates a 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
* reporting to Curriculum and e-Safety committee (and FGB where appropriate)
* reports regularly to Senior Management Team
* monitoring improvement actions identified through use of the 360 degree safe self-review tool

**Network Manager / Technical staff:**

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

* that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
* that the school meets required e-safety technical requirements of the Local Authority and LACT.
* 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
* 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
* that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher and e-Safety Coordinator for investigation and action.
* that monitoring software / systems are implemented and updated as agreed in school policies
* monitoring network / internet / incident logs

**Teaching and Support 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
* they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
* they report any suspected misuse or problem to the Head teacher and e-Safety Coordinator for investigation and action.
* 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
* pupils understand and follow the e-safety and acceptable use policies
* pupils 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 pupils should be guided to sites checked as suitable for their use and age-appropriate and that processes are in place for dealing with any unsuitable material that is found in internet searches

**Child Protection / Safeguarding Officer**

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

**E-Safety Group**

The e-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group is also be responsible for regular reporting to the Curriculum and e-Safety Committee of the Governing Body.

Members of the E-safety Group will assist the E-Safety Coordinator with:

* mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
* consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision

Pupils:

* are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
* should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s e-Safety Policy covers their actions out of school, if related to their membership of the school

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 and their children’s personal devices in the school (where this is allowed).

**Reviewed: March 2015**

**Reviewed: January 2016**

**Reviewed: March 2016**

**Reviewed: May 2017**

**Reviewed: May 2018**

**Reviewed: November 2018**

**Reviewed: July 2019**

**Reviewed: July 2020**

**Signed: Emily Day**