E-Safety Policy

Drafted by: Chris Carr (Assistant Headteacher in charge of ICT and e-safety)
Approved by Governors on: September 2014
Next Review date: Determined by Headteacher/Governing Body
Person (position, not name) to perform review: SLT responsible for ICT strategy and e-Safety.

This policy should be read in conjunction with all other policies and not as a standalone policy

The reason for the policy

All children deserve the opportunity to achieve their full potential. In our modern society this should incorporate the use of 'appropriate and safe' ICT facilities including online resources. In order for the school to maintain such an environment for learners (children and adults) all staff must be aware of the need to ensure on-line protection (e-safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

The principles of the policy

To create an "appropriate and safe environment" for users of ICT facilities including online resources the following underlying principles must be considered:

- User access levels to ICT facilities and resources (including online) should reflect the needs of the user.
- Users should know how to work safely within an online environment
- Users should be familiar with the schools "Acceptable Use Policy", "Anti-Bullying policy" , Pupil code of conduct.
- Access to internet sites, blogs, chat rooms, etc. deemed inappropriate must be restricted.
- Knowledge and training about e-safety is accessible to all members of the school community.
- Users are educated to be effective and critical users of the Internet, including the skills of knowledge location, retrieval and judgement.
- Wherever work and learning takes place using ICT facilities and resources (including online) e.g curriculum activities or professional tasks planned to support, enrich or extend learning an e-safe environment must be provided.

- Adults are up to date and know the current guidance on the safeguarding and promotion of the well-being of children and young people.
- Use of ICT facilities including internet use, by all members of the community, will be subject to monitoring and misconduct will result in disciplinary action.

These principles support our school mission statement.

The Policy

The E-safety Policy is administered by ALL staff across the school community and the responsibilities are shared. Any technology used in school (regardless of ownership) shall be governed by this policy. Students also have responsibilities under this policy also identified in the Student Acceptable Use Policy (*See Homework diary*). This policy should also be read in conjunction with the Anti-bullying policy. In support of e-safety further enhanced responsibility is undertaken as follows:

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 Governors receiving information about e-safety incidents and monitoring reports. E-safety falls within the remit of the Governor responsible for Safeguarding. The role of the E-Safety Governor will include:

- Ensure an E-Safety Policy is in place, reviewed every two years and is available to all stakeholders.
- Ensure that there is an E-Safety Coordinator who has received appropriate CEOP training.
- Ensure that procedures for the safe use of ICT and the internet are in place and adhered to.
- Hold the Headteacher and staff accountable for E-Safety

SLT

- 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 Co-ordinator.

- Any complaint about staff misuse must be referred to the e-safety coordinator (AHT in charge of ICT) at the school or, in the case of a serious complaint, to the Headteacher.
- Ensure access to induction and training in E-safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that internet filtering methods are appropriate, effective and reasonable.
- Ensure that Staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- Ensure that Pupil or staff personal data as recorded within school management system (SIMS) sent over the Internet is secured.
- Work in partnership with the LA, DFE and the Internet Service Provider and school Network manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the E-Safety Co-ordinator.

E-S afety Coordinator (AHT for ICT):

- Leads E-safety meetings.
- Work in partnership with the LA, DFE and the Internet Service Provider and school Network manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Reports to Senior Leadership Team.
- Liaise with the nominated member of the Governing Body & Headteacher to provide an annual report on E-Safety.

Network Manager / Technical staff:

The Network Manager 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 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.
- The filtering policy, is applied and updated on a regular basis and 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 Headteacher ; E-Safety Coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in School policies.

2. Curriculum Co-ordinators, Curriculum Teams, Learner Support teams and Administration teams

- Should ensure that they are familiar with The Acceptable use policies, The Anti-bullying policy and the Pupil code of conduct.
- Should inform Pupil Support Team of any misuse which may be deemed cyber bullying.
- All staff and students should be informed that Internet and e-mail use are monitored as they are the property of the school network system.
- All staff must ensure that the use of Internet derived materials by colleagues and by students complies with copyright law.
- If staff discover, or are informed of unsuitable sites, the URL (address) and content must be reported to the Curriculum Co-ordinator, Designated Child Protection Person (SLT)(or HOY) who will take action and instruct the Network manager.
- KS3 and KS4 students MUST NOT have unsupervised access to the internet at any time.
- Rules for Internet access must be posted in all rooms where computers are used.
- In lessons, instruction in responsible and safe use, along with school specific rules, should precede a student's Internet access.
- Teachers should only recommend regulated educational chat environments for student use in school and at home.
- Students MUST NOT access public or unregulated chat rooms. Where appropriate e.g. repeat offenders or otherwise, the Curriculum Co-ordinator should discuss further action with their Line Manager

- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students should be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- KS4 and KS5 Students MUST be taught how to avoid plagiarism and the penalties involved in plagiarising coursework. Should this occur you should contact the relevant Curriculum Co-ordinator.
- they report any suspected misuse or problem to the Headteacher ; E-Safety Coordinator for investigation / action / sanction
- all digital communications with students/ parents / carers should be on a professional level and only carried out using official school systems
- All staff 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.

3. Pupil Support Teams (& tutors of ALL key stages)

- Parents / Carers will be asked to sign that they have read and understood the Acceptable Use Policy in the homework diary. All tutors are required to check compliance.
- Responsibility for handling serious incidents is placed with the Pupil Support team for cases around safeguarding. An incident log will be maintained by the Pupil Support Team and regularly reviewed to spot issues or trends with regard to such offences.
- In all other incidence to Curriculum co-ordinators and DHT (Curriculum) who may need to request an intervention by the Network manager

Supplementary Guidance

- E-safety awareness can be developed via
  - ✓ One to one with E-safety officer (C Carr)
  - ✓ Attendance at scheduled CPD Inset
  - ✓ NQT Induction program
  - ✓ Departmental Guidance
  - ✓ School Website
  - ✓ School VLE (Frog)
  - ✓ CEOP trained personnel – (C Carr)
  - ✓ KS3 ICT program of study
  - ✓ Ealing Grid For Learning E-Safety Toolkit
  - ✓ BeatBullying Programme
  - ✓ Schools Newsletter
  - ✓ Updates through usual school communication channels.

- Acceptable Use Policies
  - ✓ Please view Pupils Acceptable Use policy
  - ✓ Please view Staff Acceptable Use policy

- Minor incidents of misuse by users includes:
  - copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement)
  - downloading materials or images not relevant to their studies, in direct breach of the school"s acceptable use policy
  - misconduct associated with student logins, such as using someone else"s password with permission.

- Significant issues of misuse by users include:
  - Plagiarism in coursework
  - Hacking, virus attack;
  - Deliberately accessing, printing or showing inappropriate material (this could include material accessed accidentally – but deliberately shown to others!!)
  - Harassment or infringing someone"s personal privacy.