King's Cliffe Endowed School

E-SAFETY POLICY

keeping children safe in today's electronic world

November 2016

REVIEW DATE - NOVEMBER 2018

King's Cliffe Endowed School
E-Safety Policy

1. Aims
This policy aims to give an understanding of the pitfalls and benefits in the use of the I.T., including internet and internet based technologies by all users - staff, pupils and parents. It provides some guidelines as to the type of use which is unacceptable and should be avoided, and also describes the measures which are taken within the school to assist in the development of a safer user environment.

2. Requirements
As part of the Every Child Matters agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children, young people and parents / carers is vital to the successful use of on-line technologies. This policy aims to explain how parents / carers, children or young people can be a part of these safeguarding procedures. It also explains how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

3. School Networks
The school has a network which connects all computers, staff and pupil, to each other and to the internet via a gateway. The staff computers are segregated from the pupil computers by using a different IP address subnet. The network is maintained by a third-party L.A. approved contractor. All configuration and administrative information is held by them. Internet access is provided via the L.A. approved service – the East Midlands Broadband Consortium (EMBC), whose services include accredited anti-virus, spam filtering and content filtering.

4. Pupils

4.1. Pupil Internet Use
The pupil Internet Usage Policy has been produced as an easy to understand booklet, a copy of which is given to each pupil when they first start using the computers at the school. Posters are also positioned near to computers to remind the children of key considerations when using the internet. The policy booklet is reviewed and updated in whole school assemblies in the spring term of each year so that understanding of it grows and develops as the children move through the school and they begin to take more and more ownership of it. This policy is also shared with parents annually at the beginning of each new school year. E-safety is re-visited termly with the children in school and the school council share the child friendly E-Safety policy with all children and parents annually.

4.1.1 Ofsted Inappropriate Use

Current Ofsted guidelines on e-safety inspections list the following types of site as sources of potentially inappropriate content:

- Online pornography
- Ignoring on-line gaming age ratings (exposure to violence and racist language)
- Substance abuse
- Lifestyle website (e.g. pro-anorexia; self-harm; suicide)
- Hate sites
- Grooming
- Cyber-bullying
- Identity theft

4.2. Pupil E-mail Use

Setting up e-mails is part of the ICT taught in KS2 – this is linked to E-Safety and reinforced with children termly.

4.3. Home Use

Whilst the school does not aim to control use of the internet at home, pupils will be encouraged to develop an attitude towards the internet and other forms of electronic communication which supports the aims of the school internet and e-mail policies as described in the pupils' Internet Usage Policy booklet. Parents will be encouraged to consider the potential for unmonitored internet usage at home and the various mechanisms which can be employed to help them in ensuring that their children have a safe and rich experience of using the internet.

4.4. Pupil Development

When teaching about internet and electronic communication usage, the following topics will be considered:

- inappropriate content
- cyber-bullying
- inappropriate messaging
- safe searching
- digital footprint and online reputation
- privacy
- grooming
- copyright

4.5. Incident Reporting

Where bad experiences of internet or e-mail use are encountered, pupils will be encouraged to talk about their experiences with a teacher and/or their parents. Additional coaching within the class could be employed to make pupils more aware of what to avoid on the internet, along with discussion with the pupil's parents about appropriate e-safety strategies for use both at school and at home. Where necessary, recurrences of these experiences by a pupil could be dealt with through the school's safeguarding policy.

5. Staff

5.1. Staff Internet Use

Use of the internet by members of staff is permitted and encouraged where such use supports the goals and objectives of the school.

However, the school has a policy for the use of the internet whereby staff must ensure that they:

- comply with current legislation
- use the Internet in an acceptable way

5.1.1 Unacceptable Behaviour
In particular the following is deemed unacceptable use or behaviour by staff:

- visiting internet sites that contain obscene, hateful or pornographic material
- using the computer to perpetrate any form of fraud, or software, music or video piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- creating or transmitting defamatory material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus into the school network

5.1.2 Monitoring

- The school accepts that the use of the internet is a valuable research and planning tool. However, misuse of this facility can have a negative impact upon staff productivity and the development of the children.

- The use of the internet within the classroom is encouraged, but staff should test all activity before use with children present. This is to avoid any embarrassment and avoidable exposure of the children to unsuitable material.

- In addition, all of the school's internet-related resources are provided for school purposes. Therefore, the school maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

5.1.3 Sanctions

- Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal.

5.2. Staff E-mail Use
Use of email by staff in the school is permitted and encouraged where such use supports the goals and objectives of the school.

However, the school has a policy for the use of email whereby the member of staff must ensure that they:

- comply with current legislation
- use email in an acceptable way

5.2.1 Unacceptable behaviour

- use of school communications systems to set up personal businesses or send chain letters
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered offensive or abusive, in that the context is a personal attack, sexist or racist
- accessing copyrighted information in a way that violates the copyright
- breaking into the system or unauthorised use of a password / mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-school related matters

- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus into the school network

5.2.2 Monitoring
The school accepts that the use of email is a valuable tool. However, misuse of this facility can have a negative impact upon staff productivity and the reputation of the establishment.
In addition, all of the school's email resources are provided for school purposes. Therefore, the school maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the school also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with staff.

5.2.3 Sanctions
Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal.

5.3. Social Networking
It is accepted that many people, including pupils, members of staff and parents, will be members of social networking sites (e.g. Facebook, Twitter, chat rooms, etc.). Through the school internet access policy and teaching regarding on-line use, pupils will be made aware of the dangers of social networking sites. These facilities will not be made available through school, and it will not be permitted for pupils to access social networking sites from school equipment. Through the school pupil internet access agreement parents will be advised of the desirability of monitoring their children's use of social networking. Should it be suspected that a child has been using social networking in an ill-advised manner this will be dealt with through the normal child protection procedures in place at the school.

Staff use of social networking is not prohibited, however, staff are reminded of their duty of professional conduct when communicating to other members of the profession and are advised against all contact with pupils through social networking.

5.4. Staff Use of Personal I.T. Resources
It is accepted that staff, may utilise their own I.T. resources to help them undertake their role within the life of the school. This could range from simply using a personal home computer on which to prepare lesson plans, or to undertake research; to possibly using personal equipment within the school. It is not normally desirable, or encouraged, for anyone to connect their own personal equipment to the school network.

5.5. Storage of Data
Storage of data which contains data pertaining to individuals (either pupils or members of staff) on non-school equipment is strongly discouraged. Issues of data protection and confidentiality mean that if in doubt, ensure that the data is only stored on school equipment.

5.6. Prevention of Virus Transmission
Members of staff are encouraged to ensure that their personal I.T. equipment is loaded with virus protection software updated regularly with up-to-date virus definitions. Use of good anti-virus software is essential in the protection of both personal and school I.T. equipment.

5.7. Transferring Data Between Personal & School Equipment
It is often necessary to transfer materials between personal and school equipment. The best methods are using one of the various internet based methods – such as e-mail, or the learning platform portal. Using these methods ensures that security and virus checking procedures can be applied without further measures. It is accepted that sometimes use of these methods is not possible and the use of some form of removable media device (such as a floppy disk, writable CD/DVD, or memory-stick) is

necessary. When using a removable media device it is imperative that the device is virus checked before being connected to school equipment. These devices are known to be one of the greatest causes of uncontrolled virus transmittal. Through their potential loss, they also pose the greatest risk to security and breaches of data protection – referencing the many media stories of breaches of personal data by public agencies will give numerous examples of this.

5.8. Attaching Personal Equipment to School Resources
From time-to-time it may be found greatly beneficial to the richness of learning of the pupils, for a member of staff to utilise personal equipment which they wish to attach to the I.T. resources within the school (e.g. a camera, electronic microscope, or other such devices). Before such actions are taken, the member of staff is encouraged to verify as carefully as possible any issues of compatibility with the school equipment. It also should be remembered that there are often licensing restrictions associated with software which may have to be loaded to support the peripheral device being connected. It is recommended that the I.T. coordinator is at least advised of the equipment that is being connected and any support software which is being loaded, and to which of the school computers. Remember that should any compatibility issues arise which cause malfunctioning (of software or hardware) once the device has been disconnected, this may result in the school having to make a costly support call to their support service provider – notwithstanding the inconvenience which will result in the loss of use of the computer until the issue is rectified.

6. Use of Other Electronic Information & Communication Equipment

6.1. Mobile Telephones
Pupils are not permitted to have mobile telephones on the school premises. Should a parent wish their child to carry a have telephone at school, this will only be permitted through prior agreement with the Head Teacher, and only should the circumstances presented prove exceptional.

Members of staff are requested not to use mobile telephones within the pupil areas, and when not in use should be kept in a secure location with the ringtone on silent. It will not be permissible for an individuals' mobile telephone to connect to the school network services.

7. Review
This policy will be reviewed on an annual basis, or at an earlier interval should it be found that advancements in on-line and electronic communications technologies dictate this.
This policy should be read in conjunction with the Child Protection/Safeguarding Policy.

Signed by Head Teacher: _____

Signed by Chair of Governors: _____

Date: _06th December 2016_

Review Due: December 2018