E-safety Policy
Kings Copse Primary School

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy should help to ensure safe and appropriate use.

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

The Education and Inspections Act 2006 empowers Headteachers, 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 out of school, but is linked to membership of the school. 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

The following section outlines the roles and responsibilities for e-safety 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 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.* 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
- reporting to relevant Governors committee / meeting

Headteacher

The Headteacher is responsible 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 Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. The Headteacher 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.

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
- liaises with school ICT 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
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Technician

The ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's network with an assigned username and password (although our pupils will not have passwords due to their age, while they are learning about e-safety issues)
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he / she keeps 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 / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Headteacher / Senior Leader / ICT Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

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 school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Headteacher / Senior Leader for investigation / action / sanction
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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

Child Protection Liaison Officer

Child Protection Liaison Officer should be trained in e-safety issues and be aware of the potential for serious child protection 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

Pupils

Pupils are responsible for using the school ICT systems in accordance with the Kings Copse Technology Charter (Pupil Acceptable Use Policy). Each year children in KS1 and KS2 will be expected to sign the

Technology Charter (Children in FS2 will be introduced to the charter throughout the year but will not be required to sign).

Parents/Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' e-safety sessions, newsletters and through the website.

Teaching E-Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils 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 education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT and PHSE and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced within assemblies
- Pupils should be taught to be critically aware of the materials they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the Technology Charter (pupil AUP) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- The school's Technology Charter will be posted in all classrooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Computing and Wider Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages and the school's technology charter (pupil AUP) in the use of ICT across the curriculum. In lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, e.g. using search engines, 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 these sites be unblocked so long as they have been thoroughly checked and deemed appropriate from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. As part of the curriculum, pupils will be taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. The Technology Charter enforces permission being obtained before images are shared. KS2 Children should be taught to understand the risks attached to publishing their own images on the internet e.g. on social networking sites. In practice:

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Staff members are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on the school website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or blogs

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or other removable media:

- the data must be encrypted and password protected
- the device must be password protected (encrypted memory sticks will be distributed to staff for this purpose)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Digital Communication (including email)

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)*
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, personal mobile phone numbers, text messaging or public chat / social networking programmes must not be used for these communications
- Pupils must not access any personal email accounts not administered by the school on school devices. Whole class or group email addresses will be used by classes across the school (the passwords for these accounts should not be shared with children (although they may be given passwords temporarily during a single lesson as long as the password is reset immediately after the session. When pupils are considered responsible they may be provided with an individual school email account
- Pupils should be taught about email and messaging safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

This policy was created in June 2014
To be reviewed in June 2017
GH (after EG)

Kings Copse Primary School
ICT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign Acceptable Use Agreement.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I understand that I must not use the school ICT system to access inappropriate content
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems and hardware may not be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely (memory sticks may not be used unless they are encrypted) and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidents of concern regarding children's safety to the schools e-Safety Coordinator, the Designated Child Protection Liaison Officer or Head teacher.
- I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

I have read, understood and accept the Staff Acceptable Use Agreement

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: …….

Kings Copse Primary School – Staff Social Networking Guidance

Social networking sites like Facebook, Beebo, MySpace and Twitter are becoming increasingly popular. Many of us enjoy using these sites, some even help us within our professional role, allowing us to stay in touch with other educators and share tips and ideas. However over the past few years there have been high profile cases of educators being bullied using data gathered through these sites. There have also been cases of individuals losing their jobs or even being prosecuted because of behaviour on these sites that is inappropriate. This guidance has been written to help protect us from these risks.

- Always protect yourself by making profiles on social networking sites closed or private. This limits what is publicly available. You can then share more with your friends.
- Limit the personal information you share. Remember information may be misused by others.
- Think before you post pictures or comments. Remember once it is out there it can't be taken back.
- Think carefully about confidentiality in your professional role.
- Remember it is very easy for something you share privately to be forwarded on.
- Consider your professional reputation. Don't share anything that could impact upon your reputation or the reputation of the school.
- Keep your private and professional life separate.
- It is not appropriate to become 'friends' with pupils or former pupils under 18 years of age. This kind of contact can be seen as grooming.
- Think carefully about copyright before you share images.
- Consider carefully what you say about others. Something you consider a light hearted comment may be hurtful to others when taken out of context.
- If you experience any form of bullying through these sites keep evidence and report it immediately. There is generally a report / report abuse button that you can use.

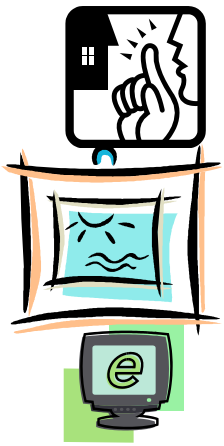
Kings Copse Technology Charter

These rules help to protect pupils and the school by describing acceptable use of technology. Remember that the school owns the computer network and can see anything you do on it. People who use technology in school in the wrong way may be stopped from using it.

I must use my own login details.

I will be polite, kind and gentle.

I will keep personal information private.



I will check it is ok before sharing pictures.

I will check with a teacher before using the Internet, downloading things or using a memory stick.

If I see something that upsets me I will tell an adult straight away.