King's School & Nursery

e-Safety Policy

Writing and reviewing the e-Safety Policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
The school will appoint an e-Safety Coordinator.

Our e-Safety Policy has been written by the school, building on the Cognita e-Safety Policy and government guidance. It has been approved by the Headteacher.

The e-Safety Policy was revised by: Sue Hallowes, 27th February 2015

It was approved by the Headteacher on: 27th February 2015

The next review date is (at least annually): February 2016

Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. The school has a duty to educate children for their use of the internet wherever that might be.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.1 We define E-Safety as:-

- ensuring student Internet use and access is appropriate and controlled.
- preventing misuse of Internet connected devices.
- ensuring students are educated on the risks carried with Internet use and how to minimise and deal with those risks.
- providing students with knowledge and resources to make decisions to ensure their safety online

1.2 Our core principles for E-Safety are:-

- The Internet and Internet connected devices provide a rich resource for supporting teaching and learning.
- Our policies seek to educate and inform students and the school community on the safe and prudent use of Internet resources
- We take a whole school, consistent approach to E-Safety, recognising that all staff should be involved and clear on their role in ensuring E-Safety education.
- E-Safety is subject to clear reporting routines and an age appropriate Acceptable Use of Technology Agreement is in place for all students.
- We recognise the need for regular training and ensure at least one member of staff takes accredited training and has a higher level of expertise.
- Our policy reflects current practice and is regularly reviewed and updated by the Lead Team and communicated to all staff.
- E-Safety is addressed within the curriculum at all ages.
- Technology in school is monitored to ensure it offers a safe access point to the Internet
- This policy should complement other school policies, in particular safeguarding policy; staff acceptable Internet and device use; data protection, anti-bullying or similar policies and student / pupil Acceptable Use of Technology Agreement.
- The E-Safety policy is dated with a review date and a named member of staff has responsibility for ensuring it is reviewed and updated on an annual basis

2.0 WHOLE SCHOOL APPROACH

2.1 We take a consistent approach to E-Safety and ensure that:

- All staff are aware of their responsibilities. E-Safety procedures are discussed in induction for new staff. The policy and procedures are discussed in staff briefings and training is provided at regular intervals.
- E-Safety is mentioned on the SDP noting current state of practice and any areas for development.
- We ensure all students understand what is meant by E-Safety through age appropriate delivery in the curriculum at all ages.
- All pupils are subject to the Acceptable Use of Technology Agreement (AUTA) which is signed by the students in Year 4 and above and discussed at the start of each new academic year.
- Parents are aware of their children's responsibilities under the AUTA and sign the agreement.
- Parents are kept up to date via a yearly E-Safety Parents Presentation.
- Awareness raising events are held, such as assemblies, parents' forums and PSCO visits.
- E-Safety is raised as part of school council discussions
- There are notices and posters giving guidance on display in key areas of the school.

3.0 ACCEPTABLE USE OF TECHNOLOGY AGREEMENT AND REPORTING

3.1 We hold an Acceptable Use of Technology Agreement (AUTA) that sets out positive guidelines for how students should use and treat technology both during the school day and outside school as school representatives.

3.2 The AUTA is delivered to all Year 4 students with a discussion of the points at the beginning of the academic year. Students are expected to sign the agreement. The agreement is presented to students joining the school outside of the start of the academic year.

3.3.The AUTA sets out guidelines for:

- appropriate and respectful use of school technology equipment and devices
- expectations and regulations for the use of students own devices in school
- expectations of behaviour if equipment is found broken or non-functional
- appropriate communications using devices in and out of school
- code of practice if students discover inappropriate or upsetting material on any device
- clear guidance on how to report any concerns

3.4 The AUTA is used positively to encourage appropriate and E-Safe behaviour and can be used alongside rewards for positive use of technology

3.5. The AUTA is supported by a clear set of age appropriate sanctions for behaviour that contradicts the agreement. Sanctions at each level should be recorded and a member of the Lead Team should be made aware of any sanctions applied to students. Records of any behaviour outside the agreement should be held, with clear description of the incident and sanctions applied

3.6 The AUTA is shared with parents and their views are welcomed and considered.

3.7 The AUTA is not intended to form the whole basis of E-Safety education, but to complement discussions and lessons on E-Safety during curriculum time and to provide a robust agreement setting out clear expectations for behaviour

3.8 The AUTA is designed to be binding for students while *enrolled* in the school and the school reserves the right to take action on behaviour that contradicts the Agreement outside of school time. In these cases the school will proceed with discretion and in partnership with parents.

3.9 Students, parents and all staff are able to report concerns and guidance for this should be set out in the AUTA

4.0 STAFF AWARENESS AND TRAINING

4.1 All staff are bound by the code of practice set out in the Cognita Schools Policy for use of Internet and mobile devices. This should be available for all staff and ensures that staff use technology safely and with adherence to safeguarding principles.

4.2 At least one member of staff should undertake accredited training. We recommend the Keeping Children Safe Online (KCSO) course provided by the CEOP. *This training is delivered online and is suggested to take 3 hours in total although it is not necessary for the course to be taken in one 'sitting'.*

4.3 The accredited member of staff should provide a higher level of expertise within the school and can guide staff in E-Safety practice and review of E-Safety policy and procedure and provide INSET guidance

4.4 E-Safety should be built into the termly programme of meetings to ensure all staff are aware of their responsibilities and for the discussion of any issues, concerns or opportunities for events or cross curricular E-Safety lessons.

4.5. There should be a clear procedure for staff wishing to report or discuss concerns relating to E-Safety or Internet access in the school. This procedure should include reporting to a member of Lead Team should be documented as necessary.

4.6 Staff responsibilities for E-Safety are: (for all staff)

- To ensure they are familiar with and fully support the student Acceptable Use of Technology Agreement
- To be vigilant when using technology as part of lessons
- To model safe and responsible use of school technology
- To provide reminders and guidance to students on acceptable use
- To report and act appropriately if they become aware of, or after any student

reports, a concern or an incident involving technology use
- To ensure E-Safety is delivered within the curriculum as appropriate to their student age range and subject area
- To contribute to and discuss E-Safety policy and to have their views heard
- To be aware of the school policy for tackling bullying and how this relates to incidents of cyber-bullying
- To be mindful of protecting data and keeping access to digital information secure by adhering to the school password policy and protecting their accounts from student access.
- To use secure portable data options including password protected or encrypted portable memory devices

5.0 E-SAFETY IN THE CURRICULUM

5.1 E-Safety should be embedded into the curriculum at all age ranges. Lessons should be well planned and resourced and there should be a number of opportunities to discuss a range of E-Safety issues.
5.2 E-Safety is expected to be covered within ICT and PSHE lessons but should not be exclusive to these subject areas and discussion of E-Safety should be explored in other subject areas both while using technology and as a topic as appropriate
5.3 Guidance on minimum coverage in each key stage:-
EYFS – safe and responsible use of technology should be modelled; Suggestions relating to ELG could include:
Communication and Language – pupils aware that they are able to communicate with others using devices – appropriate language and key words associated with technology
Physical development – safe and careful handling of technology
Personal, Social and Emotional development – sharing and cooperating while using technology
Understanding of the World – awareness of devices around us and how they are used to keep us safe, provide us with information
EYFS children should be given opportunities to learn collaboratively with devices

Key Stage 1 – Pupils should be made aware of distinction between personal, private and public information. Pupils should be taught appropriate ways to communicate when using devices and how to respond to unpleasant or distressing comments they may encounter online. They should be made aware that people they do not know are strangers including while playing online games and the importance of using 'usernames' and guarding against volunteering information. They should be taught how to respond if they are distressed or uncertain about any material they are exposed to while online or using technology.

Key Stage 2 – Issues outlined above should be addressed with the addition of: Importance of passwords and cyber security. Understanding of how cyberbullying is using technology to be unpleasant and guidance on how to respond constructively and report any thing that concerns them. Understanding of how social networks allow sharing of information and the importance of keeping information about themselves private. Understanding of how data submitted to the Internet including photographs, comments, emails etc. can be potentially accessed, altered and used by anyone. Clearer understanding of distinction between private and public information. Discussion of support networks and methods of reporting anything they are uncertain or concerned about. Understanding of spam, unsolicited and scam activity on the Internet and how accounts can be hacked or accessed by criminals.

5.4 Extra –curricular activities such as Safer Internet Day opportunities, visits from local PSCO, school assemblies should be explored but these should not represent the majority of E-Safety teaching or discussion in the academic year. They should be used to support lessons embedded in the curriculum.
5.5 Use of mobile devices during lessons is subject to control and risk management. Expectations of appropriate use of mobile devices are set out in the AUTA for students. This includes students are expected not to share digital images or videos of other students taken during lessons for any purpose other than school use.
5.5 Opportunities for peer mentoring or 'buddy' systems can be explored so that older pupils can act as role models for younger children and provide a further method for students to report concerns

6.0 INFRASTRUCTURE AND DATA MANAGEMENT

6.1 The school Internet access is subject to filtering and control and this is updated regularly
6.2 Staff are aware of how to use safe-searching options and are vigilant during lessons involving Internet access
6.3 Where available, screen watching facilities are used and staff are aware of how to utilise these resources
6.4 Passwords and digital security is in place to protect data and data is managed in accordance with the relevant DP Acts
6.5 Staff are fully aware of how to report a problem or any incidents relating to data security or Internet control
6.6 Professional communications between the school and other organisations or parents take place within clear professional boundaries, are transparent and open to scrutiny and do not share personal information with students

7.0 MONITORING, AUDIT AND POLICY REVIEW

7.1 The E-Safety policy is dated and an annual review date is stated with a named member of staff responsible for ensuring it is reviewed and updated
7.2 It may be necessary for more frequent reviews if a number of incidents are recorded.
7.3 The review procedure should be:

- An audit of effectiveness of current practice
- A review of guidance published by relevant organisations
- Amendments to be shared with all staff

Managing Internet Access

Information system security

School ICT systems security will be reviewed regularly internally and with Cognita Schools ICT Department.

Virus protection will be updated regularly.

E-mail

Pupils may only use approved e-mail accounts on the school system when a teacher is present.

Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school web site

Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully.

Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Work can only be published with the permission of the pupil and parents/carers.

- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Cyberbullying

We view cyberbullying as totally unacceptable behaviour and would deal with it in line with our Anti Bullying Policy and behaviour sanctions.

Managing filtering

If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

The e-Safety Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used to take photographs of pupils.
- Staff will not contact pupils by telephone or by networking sites. All phone contact will be via parents.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.
- Children are not allowed mobile phones in School without prior permission and if allowed should be handed to the class teacher at registration and returned by the teacher at the end of the school day

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

All staff must read and sign the “Staff Code of Conduct for ICT” before using any school ICT resource.

At Key Stage 1, access to the Internet will be by teacher demonstration with directly supervised access to specific, approved on-line materials. At KS2 parents and pupils will be asked to sign and return a computer use agreement.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a

computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, based on the materials from CEOP.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff will read and sign a copy of the e-Safety Policy.

Enlisting parents' and carers' support

The School e-Safety Policy will be available to all parents on request.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school

This policy is linked with our Child Protection Policy and Safe Guarding Policy