RATIFIED BY SMT: April 2016

BEAN PRIMARY SCHOOL
E-SAFETY POLICY

Bean School's E-Safety Policy is based on the Kent e-Safety Policy 2012 and government guidance and will be renewed annually. E-Safety at Bean School is co-ordinated jointly between the school's Designated Safeguarding Lead (DSL), the Computer Science leader and the Office Manager. The policy is reviewed annually by the governing body.

E-Safety covers issues relating to children and staff and their safe use of the internet, mobile phones and other electronic communication technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. Given that children and staff cannot be completely prevented from being exposed to risks both on and offline, children will be empowered and educated so they are equipped with skills to make safe and responsible decisions as well as feel able to report concerns. Not only must staff be aware of the importance of good E-Safety practice in class in order to educate and protect the children, but they must also be aware of how to manage their own professional reputation online and demonstrate appropriate behaviours compatible with their role.

This policy is part of the School Plan and relates to other policies – Behaviour; Personal, Social and Health (PSHE); Citizenship and Data Protection. It operates alongside Child Protection/Safeguarding Policies.

E-Safety Audit

A self-audit is completed annually by the Computer Science Lead.

Teaching and Learning

Internet is part of the statutory curriculum and a necessary tool for learning, for both staff and pupils. Pupils use the Internet widely outside of school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in school is to raise educational standards, promote pupil achievement, support the professional work of staff and enhance the school's management functions.

Enhancing Learning through the Internet

Staff will guide pupils to online activities to support the learning outcomes planned for the pupils' age and maturity, in line with requirements of the curriculum. The school's internet access will be designed to enhance and extend the pupils' learning;

- Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be shown how to acknowledge their sources, to publish and present information to a wider audience.
- Pupils will be taught how to evaluate internet content.
- The school ensure that the use of internet derived materials by staff and pupils complies with the copyright law.
- Pupils will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon as found on the school website.

Managing Internet Access

Information System Security
School ICT system's security will be reviewed annually and updated via KCC security updates. The school's broadband network includes a cluster of firewalls at each of the internet connecting modes. Advice will always be sought when needed from www.eiskent.co.uk as ICT security is a complex matter, requiring specialist support. Virus protection will be updated regularly.

E-mail
Pupils may only use approved e-mail accounts on the school system with whole class/group email addresses set up in school. They must:

- Inform a teacher immediately if they receive offensive e-mail.
- Not reveal personal details or those of others, or arrange to meet anyone without specific permission through email communication.
- Not open unknown emails.
- Whole class or group e-mail addresses may be used for communication outside school.

Also:
- E-mails to external bodies should be written carefully and authorised before sending.
- The forwarding of chain letters is not permitted.
- Staff should not communicate with pupils and parents/carers through email accounts unless an official school email account is approved by the Senior Management Team.

Publishing pupil's images and work on the school website
The school website may celebrate pupils' work, promote the school and publish resources and information for pupils and parents. Contact details on the school website include the school address, email and telephone number. Neither staff nor pupils' personal information will be published.

The school email address is – office@bean.kent.sch.uk. The headteacher will take overall responsibility and ensure that content is accurate and appropriate.

- Permission from parents/carers will be obtained before images/videos of pupils' are electronically published.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parent's permission will be obtained for pupils work to be published.
- Parents are informed of the school policy use of photographic images which outlines policies and procedures.

Social Networking

All staff are made aware of the potential risks of using social networking sites or personal publishing, both to themselves and to pupils. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable materials may affect their professional status. Social networking sites are not to be used in school by pupils or staff. Concerns regarding pupils' use of social networking, social media and personal publishing sites both in/out of school, will be raised with parents/carers, particularly if pupils are not the appropriate age to be on these sites.

Video Conferencing

Opportunities to use this 'real time' interactive technology are on the increase. If flash meetings are used, conferences will be booked as private and not made public. The conference URL should only be given to those who are to take part.

- All equipment will be switched off when not in use, and not set to auto answer.
- All equipment is stored securely on site.
- Authorisation from the headteacher is required before video conferencing can take place.
- Video conferencing will be supervised by a member of staff.

Learning Platforms

The use of the KLZ Learning Platform* continues to grow, with potential issues arising regarding content, inappropriate use and behaviour online by users. Future action will involve:

- Monitoring usage of staff and eventually pupils particularly in use of message and communication tools and publishing facilities.
- Advice of acceptable conduct and use will be given as required.

Only members of the school staff, pupil, parent/carers will have access.

Mobile Phones and Personal Devices

Mobile phones and personal devices will not be used during lessons in formal school time. Devices brought into school are the responsibility of the user and the school accepts no responsibility for loss, damage or theft. If pupils bring these items into school, they aren't to be used onsite and should be deposited at the school office first thing and collected at the end of the day.

Staff are not permitted to use their own mobile phones or devices to contact children or their families. Their phones must be switched off or on 'silent mode', and will not be used during teaching periods or duty periods. If a member of staff breaches school policy then disciplinary action may be taken.

Cyberbullying

Cyberbullying will not be tolerated as stated in the Behaviour Policy. There are clear procedures in place to investigate incidents or allegations of cyberbullying.

- All incidents will be recorded.
- All incidents/allegations will be investigated.
- Pupils, staff, parents/carers will be advised to keep a record of bullying as evidence.
- Steps will be taken to identify the bully.
- The 'bully' will be asked to remove inappropriate/offensive material.
- Service providers will be contacted to remove content if the above is not done.
- Internet access may be suspended in school.
- Other sanctions may be used in accordance with the Behaviour and Acceptable Use Policy.
- Parents/Carers will be informed.
- Police may be contacted if a criminal offence is suspected.

Managing Filtering

Broadband access will include filtering appropriate to age and maturity of pupils. Working with KCC and the Schools' Broadband team, the filtering policy is continually reviewed and breaches of the policy will be reported. Any unsuitable websites discovered by staff or pupils will be recorded and reported. The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

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. Technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. In normal situations pupils do not have mobile phones in the school. Mobile phones are not to be used during lessons or formal school time by staff. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means, will be reported and appropriate action take. Telephone contact with parents must be on the landline.

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

Staff must read and sign the 'Staff Code of Conduct' for ICT before using any school ICT resource. A record will be kept of all staff and pupils granted access to the schools electronic communications.

- Access to the Internet in Key Stage 1, will be by adult demonstration with occasional supervised access to specific approved online materials, whilst all other classes will be supervised.
- Access for Key Stage 2 pupils will be supervised. They will use age appropriate search engines and online activities will be teacher directed where necessary.
- Parents are required to sign and return a consent form giving permission for their child to access the Internet, to have photographs and work published.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources form before being allowed to access the Internet from the school site.

Assessing Risks

The school will take all reasonable precautions to ensure users access only appropriate material. However, due to the global scale and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for any material accessed or any consequences resulting from internet use. The school should audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective. The use of computer systems without permission or for inappropriate purposes could constitute as a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

Handling E-Safety Complaints

All members of the school community will be informed about the procedure for reporting E-Safety concerns. Complaints of Internet misuse will be dealt with by a senior member of staff under the school's complaints procedure. Any complaint about staff misuse will be referred to the Headteacher. The DSL will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. Reported incidents and actions taken will be recorded in the school E-Safety log and other relevant areas e.g. Child Protection Log. Parents/carers and pupils will be informed and need to work together with the school to resolve issues that may occur. Discussions will be held with the Police Safer Schools Partnership Coordinator and/or Children's Safeguarding Team, to establish procedures for handling potentially illegal issues. Any issues will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

Community use of the Internet

The school will be sensitive to internet related issues experienced by pupils out of school e.g. social networking sites and will offer/seek appropriate support advice and where necessary take action internally.

Communications Policy

Introducing the E-Safety policy to pupils

E-Safety rules are clearly posted in the computer suite and in strategic areas around the school. These are discussed with pupils regularly. Pupils are informed that network and internet use will be monitored and appropriately followed up to raise awareness and importance of safe and responsible use. A programme of training in E-Safety will be introduced based on the materials from CEOP and Miss Dorothy.com. E-Safety guidance is embedded within the Computer Science scheme of work and Personal Social and Health Education (PSHE) policy, with pupils given guidance in responsible and safe internet use, both in school and at home annually through planned assemblies across the school in the Autumn term. Safe and responsible use of the Internet and technology will be reinforced across the curriculum also throughout the year. Particular attention will be given to those pupils considered to be vulnerable.

Staff and the E-Safety Policy

A copy of this policy will be discussed with staff to ensure compliance annually.

- Staff are informed that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use are supervised by senior leaders and work to clear procedures for reporting issues.
- Staff must use a child friendly safe search engine as advised when accessing the web with pupils and when supervising pupils.
- Training will be planned for safe and responsible Internet use, both professionally and personally, for staff.
- Online conduct out of school could impact on their role and reputation within the school. Civil, legal or disciplinary action could be taken if actions are found to bring the profession/institution into disrepute.

Enlisting Parents' and Carers' Support

Parents and carers' attention will be drawn to the school E-Safety Policy in newsletters and on the school website. Parents will be signposted to E-Safety awareness training when available in the locality. The school will maintain a list of E-Safety resources for parents/carers. The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school, for e-Safety – Internet access and use of pupils work and photographs.

Based on KCC E-Safety policy guidelines. Drawn up by the Headteacher.

* CEOP – Child Exploitation and Online Protection
* KLZ - Kent Learning Zone
* BECTA – British Educational Communications and Technology Education

Ratified: April 2016
Review Date: April 2019