Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications 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.

Brookfield Junior School must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. We are aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can lead to disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that we are aware of the offline consequences that online actions can have.

The e-Safety policy is essential in setting out how the school plans to develop and establish our e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

The Headteacher and Governing Body have a legal responsibility to safeguard children and staff and this includes online activity.

- The school has appointed an e-Safety Coordinator ~ MELANIE BLEWER.
- The e-Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on the KCC e– Safety Policy and government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by the Governing Body.
- The School has appointed a member of the Governing Body to take lead responsibility for e-Safety ~ CAROLYN PRATLEY.

1.2 TEACHING AND LEARNING

1.2.1 Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside 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, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with KCC and DfE;
- access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

| Issue | | First issued |
|--------|--------------|----------------|
| Number | Page 2 of 12 | September 2000 |
| 7 | _ | Last reviewed |
| | | September 2016 |

• 1.2.4 How will pupils learn how to evaluate Internet content?

- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 MANAGING INFORMATION SYSTEMS

1.3.1 How will information systems security be maintained?

The EIS IT Security Document Library: <u>www.eiskent.co.uk?itsecurity</u>

Local Area Network (LAN) security issues include:

- Users must act reasonably e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For KCC staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Maidstone and Canterbury. These industry leading appliances are monitored and maintained by a specialist security command centre.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an antivirus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

1.3.2 How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.

1.3.3 How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

1.3.4 Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils' work can only be published with their permission or the parents' permission.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

1.3.5 How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will
 risk assess the sites before use and check the sites' terms and conditions to
 ensure the site is age appropriate. Staff will obtain documented consent from the
 Senior Leadership Team before using Social Media tools in the classroom.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

1.3.6 How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All
 members of the school community (all staff and all pupils) will be aware of this
 procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

1.3.7 How will videoconferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

1.3.8 How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are not allowed to use mobile phones and other devises during school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Staff will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

1.3.9 How should personal data be protected?

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

1.4 POLICY DECISIONS

1.4.1 How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'School Acceptable Use Policy' before using any school ICT resources.

| Issue | | First issued |
|--------|--------------|----------------|
| Number | Page 6 of 12 | September 2000 |
| 7 | | Last reviewed |
| | | September 2016 |

- Parents will be asked to read and sign the 'Responsible Use of the Internet by pupils' consent form.
- All visitors to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

1.4.2 How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only
 appropriate material. However, due to the global 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 the material accessed, or any consequences resulting from Internet
 use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

1.4.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Safeguarding Lead will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.

1.4.4 How will e-Safety complaints be handled?

- Complaints about Internet misuse will be dealt with by a senior leader.
- Any complaint about staff misuse will be referred to the head teacher.
- All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

 All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

1.4.5 How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e–Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

1.4.6 How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.

- Cyberbullying of any member of the school community will not be tolerated. (Full details are set out in the school's policy on anti-bullying.)
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
 - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
 - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
 - > Parent/carers of pupils will be informed.
 - > The Police will be contacted if a criminal offence is suspected.

| Issue | | First issued |
|--------|--------------|----------------|
| Number | Page 8 of 12 | September 2000 |
| 7 | | Last reviewed |
| | | September 2016 |

1.4.7 How will Learning Platforms be managed?

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP. When staff/pupils leave the school their account or rights to specific areas will be disabled.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

1.4.8 How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the Acceptable Use Policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times. Exceptions must be agreed by SLT.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

- If a pupil brings a mobile phone or device into school, it will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to pupils, parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside the school in a professional capacity.
- Mobile Phones and devices will be switched off or switched to 'silent' mode, and will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

| Issue | | First issued |
|--------|--------------|----------------|
| Number | Page 9 of 12 | September 2000 |
| 7 | | Last reviewed |
| | | September 2016 |

- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 COMMUNICATION

1.5.1 How will the policy be introduced to pupils?

- Pupils will be informed that network and Internet use will be monitored.
- Once a year the school will participate in e-Safety day in order to raise children's awareness of the importance of safe and responsible use of the internet through activities linked with e-Safety.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e-Safety module will be included in the PSHE, Citizenship and/or ICT themes covering both safe school and home use.
- 'Rules for Responsible Internet Use' will be posted in appropriate areas of the school.

1.5.2 How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school's pamphlet and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. (E.g. demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events such as parent evenings.)
- Parents will be requested to sign a 'Responsible Use of the Internet' agreement form.

| Issue | | First issued |
|--------|---------------|----------------|
| Number | Page 10 of 12 | September 2000 |
| 7 | | Last reviewed |
| | | September 2016 |

September 2016

BROOKFIELD JUNIOR SCHOOL e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team responsible for e-safety policy. Staff that could contribute to the audit include: DCPC, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

| Has the school a | n e-Safety Policy that com | nlies with Kent auidance | ? | Y/N |
|--|---|---------------------------|---|-------------------|
| Date of latest up | | <u> </u> | | |
| • | ety policy was agreed by g | | v. Oeptember 2 | .017 |
| | ilable for staff to access at | | | |
| | ilable for parents/carers to | | to | |
| | member of the Senior Lea | | | |
| • | | • | Diewei | |
| <u> </u> | ponsible for e-Safety is: N | | | |
| | Safeguarding Lead is: Mrs | | | |
| | ordinator is: Mrs M Blewe | | | |
| updating the sch | lders (e.g. pupils, staff and ool e-Safety Policy? | · · | | Y/N |
| - | -safety training been provi | | | <mark>Y</mark> /N |
| Do all members | of staff sign an Acceptable | Use Policy on appointme | ent? | <mark>Y</mark> /N |
| online behaviou | | | | <mark>Y</mark> /N |
| | rocedure for staff, pupils a reporting an e-Safety incic | | w when | Y/N |
| | aterials from CEOP, Childr | | n obtained? | Y/N |
| Is e-Safety traini curriculum areas | ng provided for all pupils (a | ppropriate to age and ab | ility and across | Y/N |
| Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? | | Y/N | | |
| Do parents/carers and pupils sign an Acceptable Use Policy? | | | Y/N | |
| Are staff, pupils, | parents/carers and visitors | aware that network and | Internet use is | Y/N |
| Has an ICT secu | rity audit been initiated by | SLT? | | Y/N |
| Is personal data Protection Act? | collected, stored and used | according to the principl | es of the Data | Y/N |
| Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)? | | Y/N | | |
| | tering been designed to re | | es and been | Y/N |
| Are members of | staff with responsibility for ns adequately supervised | | ork access and | Y/N |
| <u> </u> | log and record all e-Safety | • | action taken? | <mark>Y</mark> /N |
| | g Body and SLT monitorin on a regular basis? | g and evaluating the sch | ool e-Safety | Y/N |
| Issue Number 7 | Page 11 of | 12 | First issued September 2000 Last reviewed | <u> </u> |

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

e–Safety Officer, Children's Safeguards Team, Families and Social Care, Kent County Council. The e-Safety Officer is Rebecca Avery email: <u>esafetyofficer@kent.gov.uk</u> Tel: 01622 221469

Childline: <u>www.childline.org.uk</u>

Childnet: www.childnet.com

Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Kent County Council. The Children's Officer for Training & Development is Mike O'Connell email: <u>mike.oconnell@kent.gov.uk</u> Tel: 01622 696677

Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: <u>www.digizen.org.uk</u>

EiS - ICT Support for Schools and ICT Security Advice: <u>www.eiskent.co.uk</u>

Internet Watch Foundation (IWF): <u>www.iwf.org.uk</u>

Kent e-Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety

Kent Police: In an emergency dial 999. For other non-urgent enquiries contact Kent Police via 01622 690690 or contact your Safer Schools Partnership Officer. Also visit <u>www.kent.police.uk</u> or <u>www.kent.police.uk/internetsafety</u>

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): <u>www.kscb.org.uk</u>

Kidsmart: <u>www.kidsmart.org.uk</u>

Schools Broadband Service Desk - Help with filtering and network security: <u>www.eiskent.co.uk</u> Tel: 01622 206040

Schools e-Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: <u>http://en.teachtoday.eu</u>

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com