Breckon Hill ICT and E-Safety Policy Document 2016

In line with Middlesbrough School's guidance
and the UNICEF
Rights Respecting Schools Articles

This policy covers

Article 3:	The best interests of the child must be a top priority in all things that affect children
Article 17:	Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

- Mrs Diemoz (head teacher) is currently the E-Safety Co-ordinator
- Our e–Safety Policy has been written as part of a consultation process involving the Headteacher, SLT and Governing body. It builds on the advice from the Local Authority and government guidance.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- When pupils first join the school, parents/ carers will be requested to sign an Acceptable User Policy and Image Consent Form as part of the Home School Agreement. Parents/carers are able to give partial consent if deemed necessary.
- The Image Consent Form will last for the whole period the pupil is within school. Concerned parents can withdraw their consent at any time in writing to the Headteacher.
- The AUP is age specific and is reviewed at each new phase group as appropriate.

Why is Internet use important?

- 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 use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.
- Most pupils have access to the Internet outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. Many pupils only have regular access inside school and need to close the digital gap.
- The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone.

How does Internet use benefit education?

- It gives access to world-wide educational resources including museums and art galleries.
- It allows educational and cultural exchanges between pupils world-wide.
- The Internet allows vocational, social and leisure use in libraries, clubs and at home.
- The Internet and other digital and information technologies give pupils and staff access to experts in many fields.
- Professional development for staff through online access to national developments, educational materials and effective curriculum practice. Currently staff use e-learning for MSCB courses e.g. in child protection.
- The Internet allows collaboration across networks of schools, support services and professional associations.
- Through improved access to technical support including remote management of networks and automatic system updates.
- The Internet allows access to learning wherever and whenever it is convenient.
- The Internet allows an exchange of curriculum and administration data with the LA and with DFE.

How can Internet use enhance learning?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school provides regular, planned e-Safety teaching within a range of curriculum areas. There is an additional focus during e-Safety awareness week.

How will pupils learn how to evaluate Internet content?

- As Pupils move through Key Stage 2, they are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

How will information systems security be maintained?

- Virus protection is installed on all school computers/laptops and configured to receive regular updates.
- The security of the school information systems and users is reviewed regularly.
- Personal/sensitive data sent over the Internet or taken off site will be encrypted e.g. via zipped password protected documents, encrypted portable storage devices and encrypted laptops.
- Portable media may not used without specific permission and will need to be virus checked prior to use on school devices.
- Software, including browser tool bars, should not be installed on school computers/laptops without prior consent from the Headteacher. An up to date record of all appropriate licences for all software is kept within school.
- Files held on the school's network will be regularly checked for viruses, Malware and Spyware.
- The network manager and technical support provider (Advantex) will review system capacity regularly and report any concerns to SLT.
- As pupils move into upper Key Stage 2, they will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The school has agreed procedures for starters and leavers. A log is kept to identify who ICT equipment has been assigned to and staff are asked to sign equipment in and out if it has not been allocated to them.
- A member of SLT will ensure that the ICT technical support team is informed promptly of any member of staff joining or leaving the school. With regards to leavers, the ICT support team will be asked to disable/remove them in a timely manner.
- All staff/pupils will be reminded to follow the agreed format for creating passwords (e.g. mixtures of letters, numbers and symbols) and the need to keep passwords secure.
- All servers, wireless systems, network components and cabling are securely located and physical access is restricted.

How will filtering be managed?

- The school works with the technical support provider (Advantex) to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable content when using the internet/email, staff will report the URL/email to the school's e–Safety team who will follow the agreed school procedures.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP. A flow chart to assist in how this can be done is available on the school area of the council website.
- The school will ensure that the infrastructure/network are as safe and secure as possible. The filtering system, Sonic Wall, is supplied by Advantex The filtering system offers a high level of protection that meets Internet Watch Foundation (IWF) standards. However the nature of the Internet makes it impossible to ensure that all inappropriate material is blocked.
- The school's access strategy is designed by teaching staff to suit the age and curriculum requirements of the pupils, with advice from network managers/ technical support providers.
- Children will always be supervised as part of a class or group by a member of staff when using computer equipment in school.
- In addition to the filtering solution, the school has procured an e-Safety product "e-safe" to further protect staff and pupils against cyber-bullying (online bullying). This also enables the school to be proactive in educating pupils in e-Safety.

How will remote access be maintained?

- When using any type of remote access to school data, staff are required to adhere to the school agreed password policy. All staff sign an AUP regarding access to school data.
- Third parties will only be given remote access with prior authorisation from the Headteacher and governing body.

How should personal data be protected?

- Personal/sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Under the Data Protect Act (1998) all schools must comply with the eight enforceable principles of good practice. Data must be; Fairly and lawfully processed, Processed for limited purposes, Adequate, relevant and not excessive, Accurate, Not kept longer than necessary, Processed in accordance with the data subject's rights, secure and not transferred to other countries without adequate protection
- All data should be kept secure and staff will be informed of what they can and cannot do with data.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts (for example; gmail/live@edu/office 365).
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Generic class email address should be used for communication outside of the school to protect pupils' identities.
- Pupil access in school to external personal e-mail accounts is not permitted.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- School uses GCSX email to report safeguarding issues to the Vulnerable Children Department and Admissions Team.
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.
- All digital communications should be professional in tone and content.
- Email users within school are made aware, through training, that emails are covered by the Data Protection Act (1990) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- Staff and pupils are made aware, through the AUP, that all e-mail communications maybe monitored.

How will published content be managed?

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The head teacher has overall editorial responsibility and ensure that content is accurate and appropriate.
- The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The school website will adhere to the statutory requirements as set out by the DfE.

Can pupils' images or work be published?

- Images that include pupils will be selected carefully and will not provide material that could be reused. The school Image Consent Form ensures that all of the following points are covered;
- Pupils' full names will not be published (e.g. Websites and Newsletters), particularly in association with photographs. If a photograph of an individual is used then it should not include the individual's full name in the accompanying text or photo caption. If an individual is named in the text, then no photograph of that person will be included. If a group photograph is published then a general caption should be given e.g. School trip.
- Written permission from parents/carers is obtained as part of the school admission procedures otherwise images of pupils cannot be taken and published. Verbal consent must not be accepted under any circumstance. School staff will also be asked if they wish their photo to be used.
- Photographs, images and videos are regarded as personal data under the Data Protection Act (1998). Photographs and videos will only be taken using school equipment and only for school purposes.
- All staff/pupils are educated about the risks of taking, using, sharing, publishing and distributing digital media.
- If an individual supplies the school with a photograph, they can remove permission for use at any time in the future.

- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

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

- Breckon Hill allows access to social networking sites only for teaching purposes.
- Newsgroups are blocked unless a specific use is approved.
- Pupils are 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 e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are educated not to place personal photos on any social network space. They are taught to consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers are advised not to run social network spaces for student use on a personal basis.
- Pupils are educated on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.
- Students are advised not to publish specific and detailed private thoughts.
- As part of the Acceptable User Policy, staff are asked to ensure that any personal social networking sites / blogs etc that they create or actively contribute to are not confused with their professional role. They are asked not to create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring their professional role, the school, or the Council, into disrepute.

How will videoconferencing be managed?

The equipment and network

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer. Breckon Hill uses Skype as the facility to work both between classes and externally where approved.
- Videoconferencing contact information should not be put on the school Website.
- The programme is password protected on the i-boards in school.

Users

- Parents and carers must agree for their children to take part in videoconferences outside of school.
- Unique log on and password details for the educational videoconferencing services are only issued to members of staff and kept secure.

Content

- Videoconferencing is supervised appropriately for the pupils' age.

- Dialogue is established with other conference participants before taking part in a videoconference.

- 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. Copyright, privacy and Intellectual Property Rights(IPR) legislation will be breached if images, video or sound are recorded without permission.

- Approval from the Headteacher will be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.

- Pupils using video conferencing equipment should be supervised at all times.

- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'stop' or 'hang up' the call.

How can emerging technologies be managed?

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

How will mobile devices be managed?

- Staff are made aware, in the AUP, that they are responsible for safeguarding school ICT equipment (such as laptops) and should take all precautions necessary to prevent theft, loss or damage of such items and prevent unauthorised access.
- Removal of mobile technology from school premises is only permitted with prior authorisation from the Headteacher and the equipment taken is logged. Any equipment taken is for school use only.
- Children are not permitted to bring personal mobile devices into school, unless prior authorisation by the Headteacher is gained. Any unauthorised devices (e.g. mobile phones) will be taken from the child and stored in a secure location until the end of the day. Staff then contact parents.
- Staff are not permitted to use mobile phones during lesson times, unless prior consent is given from the Headteacher. Staff can use their mobile phones on designated break times away from any children

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure. The e-safe system allows for individual log-ons to be monitored and black-listed words flag up an incident to the SLT.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with Middlesbrough Children's Safeguarding Board (MSCB) to establish procedures for handling potentially illegal issues for which the police will need to be involved.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken and kept for reference.

How is the Internet used across the community?

- The school liaises across the Co-operative Trust to establish a common approach to e-safety.
- The school is sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- There are clear procedures in place to support anyone affected by cyberbullying.
- All incidents of cyberbullying reported to the school are recorded using the school's CPOMs system.
- There are clear procedures in place to investigate incidents or allegations of cyberbullying. Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence.
- The school has procured an e-Safety product "e-safe" to further protect staff and pupils against cyber-bullying (online bullying). This also enables the school to be proactive in educating pupils in e-Safety.
- Outside agencies such as NSPCC are invited into school to promote e-safety including staying safe using mobile phones with apps such as Snapchat, Instagram, Facebook etc

How will Internet access be authorised?

- The school maintains a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the Acceptable Use Policy before using any school ICT resource.
- From Reception to Year 2, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- KS2 students must apply for Internet access individually by agreeing to comply with the e-Safety Rules.

- Parents are asked to sign and return a consent form for pupil access on entry to KS2 and at admissions for KS2 pupils.
- Parents are informed that pupils will be provided with supervised Internet access.

How will Learning Platforms and Learning Environments be managed?

- School uses Education City as a Learning Platform children can use both in and outside of school. Home access is at a cost to school and is only granted when children are actively using the platform

How will risks be assessed?

- The school audits ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks are reviewed regularly.
- 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 MBC can accept liability for material accessed, or any consequences resulting from Internet use.

How will parents' support be enlisted?

- Parents' attention is drawn to the School e–Safety Policy in the school brochure and on the school website.
- Interested parents will be referred to relevant organisations
- A partnership approach with parents is encouraged. This includes parent sessions with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events. The Parent Support Advisor Team work with individual parents to support specific issues.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is made available to parents.
- Information and guidance for parents on e–Safety is made available to parents in a variety of formats.

How will the policy be discussed with staff ?

- The e–Safety Policy is discussed with all members of staff at the start of year and in induction meetings.
- Staff should be aware that Internet traffic is 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 the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally is provided.
- To protect all staff and pupils, the school implements Acceptable Use Policies.

How will the policy be introduced to pupils?

- E-Safety rules are posted throughout school
- An annual e–Safety training programme is in place to raise the awareness and importance of safe and responsible internet use.
- Pupil instruction in responsible and safe use precedes Internet access.
- An e–Safety module is included in ICT curriculum covering both safe school and home use and is promoted in a cross curricular manner.
- All users are informed that network and Internet use will be monitored.
- e–Safety training is part of the transition programme across the phases
- Safe and responsible use of the Internet and technology is reinforced across the curriculum. Particular attention is given where pupils are considered to be vulnerable.