Brightlingsea Junior School

E-Safety Policy

E-safety at Brightlingsea Junior School

Introduction

Technology and communications are rapidly changing and becoming more sophisticated, with this change comes new ways of being unsafe and feeling threatened. E-safety has become a very important issue that is essential to address in school throughout different areas of the curriculum, to ensure that all children and adults remain safe and in control when using technology. This could be either, computers and mobile devices having access to the internet or through mobile telephones.

Aims

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they feel unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.
- How to take the necessary measures to block and delete accounts, messages and people.

Roles and Responsibilities

All the adults that are involved in the life of the school; whether governors, teaching staff, support staff, technicians or volunteers have roles and responsibilities that are associated with e-safety as well as all pupils that come into contact with computer technology.

Governors
The Governors are responsible for the approval of the E-Safety Policy and reviewing its effectiveness.

The Headteacher
The Headteacher is responsible for ensuring the safety, including e-safety, of the members of the school community. The day-to-day managing of e-safety will be delegated to the E-Safety and ICT Co-ordinators.

E-Safety and ICT Co-ordinators
The E-Safety and ICT Co-ordinators will:

- take day-to-day responsibility for e-safety issues and have a leading role in establishing and reviewing the school's e-safety policy and other related documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and will provide training and advice for all staff
- liaise with the Local Authority and liaise with school ICT technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Technical Staff

- The Network Manager/ICT Technician is responsible for ensuring that:
- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's network through a properly enforced password
- their knowledge is up-to-date with relevant e-safety technical information and guidance in order to carry out their role effectively
- monitoring software/systems are implemented and up dated regularly.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they stay up-to-date with current e-safety matters, policies and practice
- they report any misuse or problems to the E-Safety Co-ordinator/Headteacher for further investigation
- e-safety issues are embedded throughout the curriculum
- pupils follow the E-Safety Policy
- 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.
- All staff should adhere to the guidelines set out in the HR Staff Code of Conduct policy
- All staff are expected to read and agree the Employee Agreement for the use of School digital technologies (Appendix 2)

Pupils

- All children should read and agree the **Pupil contract for safe computer and internet use (Appendix 1)**
- The school expects all children to be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use
- When using the Internet children should not deliberately seek out offensive materials. Should any child encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site
- Children should not to use any rude or offensive language in their digital communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for digital communication and will be expected to follow them
- Children must ask permission before accessing the Internet and have a clear idea of why they are using it
- Children must not access other people's files unless they have permission to do so
- Computers, laptops and netbooks should only be used for school work and homework unless permission has been given otherwise
- No program files may be downloaded from the Internet to the computer, to prevent corruption of data and to avoid viruses
- No programs on CD Rom or flash drive/memory sticks should be brought in from home for use in school. This is for both legal and security reasons. Homework completed at home may be brought in on a memory stick, but will be virus scanned by the class teacher before use.
- No personal information such as date of birth, phone numbers and addresses should be given out and no arrangements should be made to meet an unknown person via the Internet/email

- Children consistently choosing not to comply with these expectations will be warned, and may be denied access to Internet resources. They will also be subject to the general disciplinary procedures of the school.

Parents/Carers
Parents/carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They must be aware of the schools AUP and agree to it.

Education and Training
All children will receive planned e-safety lessons throughout ICT; these lessons will be regularly revisited and revised to suit new technologies in and out of school. Key messages will be delivered through a variety of assemblies to ensure all children are aware of the matter. They will also be made aware to question the validity of the information they find on-line.
Parents will be kept informed with regular e-safety updates and they will also have the chance to ask questions regarding e-safety at meetings which are held.
All staff will receive regular training regarding e-safety and an audit of their e-safety needs will be carried out. All new staff will receive e-safety training as part of the induction process, ensuring they are fully aware and understand the E-Safety Policy and the AUP. The E-Safety Co-ordinator will attend regular updates provided by the Local Authority or other training schemes and disseminate relevant information back to staff. The E-Safety Co-ordinator will provide guidance for any member of staff that seeks it.

Technical
Brightlingsea Junior School receives a filtered broadband service through the broadband connectivity. This service is intended to stop users from accessing any material that would be regarded as inappropriate for the learning environment or illegal. The service is provided the LA.
All personal data will be stored accordingly to the Personal Data Act 1998. Staff must use personal data on secure password protected machines and other devices, ensuring that they 'log off' at the end of any session. This will then minimise any chance of the data being seen by others. Any personal data that is stored on a USB device also needs to be password protected or encrypted. Devices must have virus and malware checking software. Any data must be securely deleted from any devices.

Curriculum
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
During 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the pupils visit.
It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg, weapons, which could be part of a study on the Roman Army so that they can be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

Use of Digital Video and Images
The developments of digital images and videos have significant benefits within the curriculum and enhance learning. Images and videos can either be taken by staff and pupils for educational

purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.
When using digital images, staff should inform and educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet, eg on social networking sites.
Staff are allowed to take digital/video images to support educational purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
Care should be taken when capturing images/videos in that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute.
Pupils full names will not be used anywhere on the website or in blogs and particularly not associated with photographs.
Written permission is provided to every parent/carer when their child that starts the school asking whether they allow their child to be photographed. It is the parents'/carers' responsibility to inform the school if they do not wish their child's image to be published on any externally accessible media; otherwise it is assumed that they give their consent.
Brightlingsea Junior School complies with the Data Protection Act 1998 in regards to digital images and videos.

Misuse and Infringements

All users of computers and hand held devices will be made aware of what is acceptable or not by the Employee Agreement. If unacceptable use is carried out, sanctions will be put in place and the reporting of these offences are outlined.
It is expected that all users will be responsible and safe users of ICT and will follow the E-Safety Policy. However, at times an infringement of the policy may occur whether through carelessness or, very rarely, deliberately.

The correct procedure is in place for reporting illegal activity and all staff are aware of who to speak to in the first instance. This being, the E-Safety Co-ordinator, who will then investigate the matter. If the matter is of a serious nature then the Child Protection Officer/Headteacher will be informed, who will take the matter further. All children will be made aware of the importance to report any incident to either an adult at school who they can trust or the 'Report Abuse' button that is present on the school website, regarding any incidents that may occur outside of school.

Monitoring, Review and Policy Ownership

Brightlingsea Junior School seeks to work in partnership with parents/carers to provide effective e-safety. Parents/carers need to know that the school's e-safety programme will complement and support their role as parents/carers and that they can be actively involved in the implementation of the school's policy.

Appendix 1 – Pupil contract for safe computer and internet use:

BRIGHTLINGSEA JUNIOR SCHOOL

Acceptable Use Agreement

In order to keep ourselves and others safe I agree to the following:

1. I will use the school computers, Internet, and all our technological equipment sensibly.
2. I will ask permission before entering any website, unless my teacher has already approved that site.
3. I will not enter chat rooms or leave messages on bulletin boards.
4. If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
5. I will never insert my personal details, home address, or telephone numbers on the Internet or in an e-mail.
6. I will only e-mail or message people or open e-mails from people I know, or my teacher has approved.
7. I will always be polite and use appropriate language when sending e-mails or messaging.
8. I will not look at or delete other people's files without their permission.
9. I will only use my own username and password to access the computer network.
10. I know that the school may check my computer files, monitor the Internet sites I visit and filter the contents of my e-mails.
11. I understand that if I deliberately break these rules, I could be stopped from using the school network and accessing the Internet.

Full name……

Date ……

Appendix 2 - Employee Agreement for the use of school digital technology

Prohibited communications

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene, sexually explicit or pornographic;
- Defamatory or threatening;
- In violation of any license governing the use of software;
- Engaged in for any purpose that is illegal or contrary to the school's policy or interests.

Personal use

The computers, digital technologies and services provided by the school are primarily for educational use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their educational purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Access to employee communications

The school reserves the right to routinely monitor employee communications directly, e.g., telephone numbers dialled, sites accessed, call length, and time at which calls are made, for the following purposes:

- Cost analysis
- Resource allocation;
- Optimum technical management of information resources
- Detecting patterns of use that indicate employees are violating school policies or engaging in illegal activity

The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies.
Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.
Under no circumstances should pupil–named data be transmitted over the Internet or email. The school office has use of encrypted data systems for this purpose.

Software

To prevent computer viruses from being transmitted through the school's computer system, unauthorised downloading of any unauthorised software is strictly prohibited. Only software

registered through the school may be downloaded. Employees should use virus trapping software on any home computer that is used to download planning or other information onto the school computers. Employees should contact the headteacher if they have any questions.

Security/appropriate use

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorisation has been granted by school management, employees are prohibited from engaging in, or attempting to engage in:

1. Hacking or obtaining access to systems or accounts they are not authorised to use
2. Using other people's log-ins or passwords
3. Breaching, testing, or monitoring computer or network security measures

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Participation in online forums

Employees should remember that any messages or information sent on school-provided facilities to one or more individuals via an electronic network - for example, Internet mailing lists, bulletin boards, and online services - are statements identifiable and attributable to the school.

The school recognises that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a news group devoted to the technical area.

Violations

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible disciplinary action, legal action, and criminal liability.

Advice to staff on the use of social networking sites

There have been many issues with Facebook and other social networking sites in schools over the last couple of years. The internet is a public domain not a private one and staff in schools must be aware that information which they share and post is accessible to the public at large. It is therefore particularly important that staff do not name or discuss individuals – children, staff, parents or governors – on social networking sites. To do so would constitute a serious breach of confidentiality and data protection procedures.

All school staff, particularly teachers, risk exposure in the press and potential complaints to headteachers, governors and the Local Authority when information posted on the Internet suggests behaviour which compromises their position as role models to pupils.

As a school we therefore offer the following advice to staff:

1. Ensure that you do not post any photographs on the Internet which could give cause for embarrassment.
2. Do not post any comments which could compromise your own integrity or which could bring the school, your colleagues, parents or the school community into disrepute.
3. Do not discuss school matters, including comments about children, staff, parents or governor on social networking sites.
4. Check that you are happy with the privacy levels on your pages and review these settings regularly.
5. You are very strongly advised **not to allow children to become 'friends'** (even if they are no longer in the school) on these sites. This is because it is deemed to be inappropriate to encourage out-of-school relationships with children and because of the nature of some of the likely content of material on sites used by adults.
6. If a complaint is received about a member of school staff then this will be dealt with under the school's disciplinary procedures and in consultation with Essex County Council's HR Team.

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of Brightlingsea Junior School's computers, digital technologies and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that violations of this guideline on appropriate use of the e-mail, Internet systems and participation in social networking sites may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of e-mail, Internet systems and participation in social networking sites may reflect on the image of Brightlingsea Junior School to our pupils, parents, governors and suppliers and that I have responsibility to maintain a positive representation of the school.

Signature of employee: ……..

Printed name of employee: …….

Date: ……..