Bowdon Preparatory School

Acceptable Use of ICT and eSafety Policy

This policy sets out the school's expectations for classroom practice and the responsibilities of different staff in contributing to an outstanding learning environment it should be read in conjunction with the following policies.

School's Aims	Internet code of conduct for pupils – EY and Infants
Safeguarding Policy	Internet code of conduct for pupils Juniors
Acceptable Use of ICT - Code of conduct for staff	Positive Behaviour Policy
Data Protection Policy	Anti-Bullying Policy

eSafety Officer: **Sophie Hughes**

IT Manager: **Claire Corrigan**

Introduction

Our e-Safety Policy is a revision of the existing Acceptable Use Policy, building upon government guidance, to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. It has been agreed by the senior management team and approved by governors.

The Internet is now considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning. This policy considers the use of both the fixed and mobile internet, PCs, laptops, tablets, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

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 information systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

The school will ensure that all members of the school community are aware of the Acceptable Use and e-safety policy and the implications for the individual. E-safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

We believe that it is really important for children to stay safe online. Using the Internet sensibly is something that we encourage all children to do and at all times, whether in school or at home.

Aims

At Bowdon Prep School we believe that educating our children about being safe on-line is very important. As part of our Computing curriculum all children from Foundation Stage to Year Six follow our Online Safety Scheme of Work focusing on identifying some of the risks about being on-line and how to keep themselves safe. In school we have clear rules about using the internet and these are displayed in every classroom

The computer system is owned by the school and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's internet policy has been drawn up to protect all parties, - the pupils, staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

Staff and pupils accessing the internet must accept and comply with the following guidelines:

- All internet activity should be appropriate to the pupil's education, staff professional activity or appropriate personal use outside of teaching time.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT Systems, or activity that attacks or corrupts other systems is forbidden.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- Use for personal financial gain, gambling, terrorist or political purposes or advertising is forbidden.
- Copyright materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.

- As e-mails can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the internet to access inappropriate material such as pornographic, racist, terrorist or offensive material is forbidden.
- Pupils can only use the internet in school whilst supervised by a member of staff.
- Pupils must finish their session on the internet as soon as they are told to do so.
- Pupils may only visit websites which have been agreed by the teacher.

Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Headmistress, with the support of the Senior Management Team, aims to embed safe practise into the culture of the school. The Headmistress ensures that the policy is implemented and compliance with the policy monitored.

Our e-Safety Officer and IT Manager ensure they keep up to date with e-Safety issues and guidance from DfE and through organisations such as The Child Exploitation and Online Protection (CEOP). They also ensures the Headmistress and senior management are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. Central to this is Internet fostering a “No Blame” culture so pupils feel able to report any bullying, abuse or inappropriate materials.
All staff should be familiar with the school’s Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network.
- Safe use of school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones, tablets and digital cameras.
- Publication of pupil information / photographs and use of website.
- Cyberbullying procedures.
- Their role in providing e-safety education for pupils.

During whole school staff INSET days, staff are reminded / updated about eSafety matters at least twice a year.

Protecting Children

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the Internet may give children access to undesirable information or images. Children are regularly reminded that should they encounter inappropriate material on line they must immediately:

1. Turn off the screen.
2. Report immediately to the teacher or supervising adult who will record the URL and other details.
3. Refrain from describing or encouraging others from accessing the site either directly or through a search engine.

Should a child or teacher encounter unsuitable material, this will be reported as a matter of urgency by the

Use of a Filtered Service: Access to the Internet is provided through a filtered service. No filtering service is 100% effective; therefore all children's use of the Internet is supervised by an adult.
Planned Activities
Use of the Internet is a planned activity. Aimless surfing is not allowed. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

School Systems

Internet access in the school is provided via a BT Business broadband link. Web filtering appropriate to the age of the pupils has been applied on all PC's, to ensure pupils are not exposed to inappropriate content, including extremist material. A suitable virus protection system has been implemented through the school and is installed on all computers in school. This software will be automatically updated regularly. Portable media may not be brought into school without specific permission and a virus check. Pupil access to the Internet will be by adult demonstration or directly supervised access to specific, approved on-line materials. Instruction in responsible and safe use by pupils will precede Internet access. The safe search facility has been applied on Google for all devices and a child-friendly search engine is set as default on all PC's in the ICT suite.

Curriculum

As part of the curriculum, pupils will be made aware of the guidelines for the acceptable use of the Internet and what is not acceptable. These guidelines for acceptable use will be clearly on display in all areas of the school where Internet access is available. All pupils will be given clear objectives when using the Internet. Where Internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the school. Training is available to staff in the evaluation of Internet materials.

Curriculum activities that involve the use of the Internet for gathering information and resources will develop pupil skills in locating and evaluating materials. Pupils will be taught how to validate materials they read before accepting their accuracy. Other techniques for research will be developed through the use of appropriate web searches and school approved sites. Where materials gathered from the Internet are used by pupils in their own work, they will be taught to acknowledge the source of information used. The school will ensure that the use of Internet materials by staff and pupils complies with copyright law.

Cyber Bullying

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or e-mails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (eg MySpace) or online diary (blog)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail (such as 'Happy Slapping' videos)

There are many types of cyber-bullying. Although there may be some of which we are unaware, here are some of the more common:

- Text messages – that are threatening or cause discomfort – also included here is “Bluejacking” (the sending of anonymous text messages over short distances using “Bluetooth” wireless technology.
- Picture/video-clips - via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls – silent calls or abusive messages; or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
- Emails – threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
- Chat room bullying – menacing or upsetting responses to persons (children, young people or adults), when they are in web-based chat room.
- Instant messaging (IM) – unpleasant messages sent while children conduct real- time conversations online using MSM (Microsoft Messenger) or Yahoo Chat; although there are others.
- Bullying via websites – use of defamatory blogs (web logs), personal websites and online personal “own web space” sites such as Bebo (which works by signing on in one’s school, therefore making it easy to find a victim) and Myspace – although there are others.

It should be noted that the use of ICT to bully could be against the law. Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the Harassment Act 1997 or the Telecommunications Act 1984 for example. It should be noted that the use of the web, text messages, e-mail, video or audio to bully another pupil or member of staff will not be tolerated. Full details can be found on the Anti bullying Policy.

Preventing Radicalisation and Extremism

Appropriate web filtering has been applied to the school network to ensure our pupils are safe from terrorist and extremist material. The school values the "core values" of a democratic society, including freedom of speech, however, all rights come with responsibilities, and free speech or beliefs designed to manipulate the vulnerable or which advocate harm or hatred towards others will not be tolerated.

Radicalisation will be viewed as a safeguarding concern and will be referred to the appropriate safeguarding agencies.

Emails

Curriculum activities that involve the use of e-mail will be through the use of Purple Mash and/or class or group webmail accounts that are controlled by the school. All e-mail communications sent by members of staff that relate to the school will be through authorised, school controlled webmail accounts. The use of individual pupil personal accounts will not be permitted through the school system. Any e-mail sent to an external account will be authorised by the school, before sending, following the same procedure used for letters written on school headed notepaper. Pupils will never reveal personal details of any member of the school community in e-mail communications.

Social Media and Portable Devices

The use of online chat rooms, social networking sites, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the pupils. The use of mobile phones will not be permitted during lessons or formal school time. This is to avoid the possibility of the sending of abusive or inappropriate text messages. Staff must ensure that personal devices are switched off during the school day.

The School Website

The school website is maintained and kept up to date. The headmistress ensures that the content is accurate and appropriate to the needs of the school community. No personal information about any member of the school community will be published on the website. Written permission from parents or carers will be obtained before photographs of pupils or pupil names are published on the website. Only first names of pupils will be published and these will never be published in conjunction with photographs. Any photographs published will not allow individual pupils to be identified.

Consent Forms

A consent form, which covers permission to access the Internet, will be issued to parents and carers to cover the academic year. This will contain the acceptable use guidelines and details of the school e-safety policy. Parents and carers will be required to sign the consent form and where appropriate pupils will also be required to sign an acceptance of both the acceptable use guidelines and the e-safety policy. The signed consent form must be returned to the school for pupil access to the Internet to be permitted. Pupils will be informed that Internet use will be monitored. Pupil access may be withdrawn if the acceptable use guidelines are not adhered to.

All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school e-safety policy. All staff will need to sign a copy of the *Staff Information Systems Code of Conduct* before using any Internet resource in school. Staff will be made aware that Internet traffic can be monitored and traced to the individual user and professional conduct is essential. Staff development in safe and responsible Internet use will be provided as part of the continuing professional development programme.

The school will keep an up-to-date record of all staff and pupils who are granted Internet access.

Websites for children

KidSmart - Learn more about the Internet and how to be a SMART surfer

ThinkUKnow - Advice on online safety

CBBC Stay Safe - E-Safety games and songs

Childnet - Working to make the Internet a safe place for children

DigiDuck's Big Decision - A story about online friendship and making the right decisions (KS1)

Adventures of Smartie The Penguin -A story about asking for help when using the Internet (KS1)

Digizen - Become a responsible digital citizen

The Adventures of Kara, Winston and the SMART Crew

Websites for parents

- **Safe Network -** Guidance on helping keep children safe online
- **The Parents' and Carers' guide to using the Internet**
- **CEOP YouTube Channel (for Parents/Carers)**
- **Digital Family - o2**
- **Keep Safe Online - Cyberbullying**
- **Keep Safe Online - Glossary of Terms**

Monitoring and Reporting

The eSafety Officer will ensure that the e-safety policy is implemented and compliance with the policy monitored. Staff and pupils should be aware that some material available on the Internet is inappropriate for specific age groups and could therefore cause risks of harm. Every teacher needs to be aware of the risks posed by online activity, including that of extremist and terrorist groups.

Methods to identify, assess and minimise risks will be reviewed regularly. The school will take all reasonable precautions to ensure that pupils access only appropriate material. However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Where unsuitable content is encountered, staff and pupils should follow the school procedures for such events. Unsuitable URL addresses will be reported through the IT Manager. Pupils must report unsuitable material, including e-mail content, immediately to a teacher. The teacher will then ensure that the reporting procedures are followed. Parents will be informed of such incidents sensitively to avoid undue distress.

Where incidents occur due to non-compliance with the school e-safety policy these will be reported to the ICT Manager and if necessary the eSafety Officer. Any issues relating to staff misuse must be referred to the Headmistress. Should it become necessary to prohibit the use of internet resources for a pupil, then parents or carers will be involved so that a partnership approach can be used to resolve any issues. This could include practical sessions and suggestions for safe Internet use at home.

Policy Dissemination, Monitoring and Evaluation

All members of staff and Governors will receive a copy of this policy. Copies may be reviewed by parents. This policy will be reviewed, evaluated and updated annually to assess its relevance and effectiveness.

Date of update	(U) Updated (R) Reviewed by	How was updated disseminated	Parents informed	Policy on website
Sept 2016	C. Corrigan (U)	Staff briefing – email – all staff to familiarise and action	Yes	Yes
Oct 2016	H. Gee (R)			
Feb 2017	H. Gee (U)	Staff Briefing	Yes	Yes