Beechlawn School

E Safety

and

Acceptable Use Policy

2014

1 What is E-Safety?

E-Safety is short for Electronic safety. It encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. E-safety highlights the need of the school, staff and parents to educate children and young people about the benefits, risks and responsibilities of using information technology.

- E-Safety concerns safeguarding children and young people in the digital world.
- E-Safety emphasises learning to understand and use new technologies in a positive way.
- E-Safety is less about restriction and more on education about the risks as well as the benefits so pupils can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

1.1 Professional Development for Staff

Staff are the first line of defence in E-Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to illegal activity. Staff should avail of training and support provided in school to determine what action is appropriate including when to report an incident of concern to Mr Corrigan the school Designated Teacher for Child Protection or the Deputy Designated Teacher Miss Holmes or in their absence the Principal.

They may inform Mr Briggs, the C2K Administrator. Additional support and advice is available from C2k, Social Services or the PSNI if required in school. E-Safety training is an essential element of staff induction and E-Safety shall be reviewed annually will all staff alongside Child Protection training in school.

1.2 Education of Pupils

The Internet is an increasing feature and an integral part of everyday life. It is an essential element for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. School Internet access is designed for pupil use and includes filtering by C2k, which shall be appropriate to the age of pupils.

In School pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. They will be taught to be "Click Clever, Click Safe":

- **Zip it** (never give personal data over the internet)
- **Block it** (block people you don't know)
- **Flag it** (if you see something you don't like flag it up with someone you trust).

Throughout each year in ICT pupils shall be taught specific lessons on E-Safety for school and home to continually remind them of the importance of keeping safe. These resources have been distributed by E Hanna, ICT Coordinator.

Should teaching staff want to avail of further resources - Child Exploitation and Online Protection (CEOP) resources are a useful teaching tool for all Key Stages looking at Internet safety and can be usefully incorporated into a PD/MU/LLW or ICT programmes. See also ***www.thinkuknow.co.uk***

One more source of information is Childnet International is a non-profit organisation working to "help make the Internet a great and safe place for pupils". Childnet have produced many materials for pupils, parents and staff; to support the teaching of E-Safety to pupils of all ages. Their materials are available to access online or order from ***www.childnet.com.***

1.3 Risk Assessments

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become "Internet-wise" and ultimately good "digital citizens".

As required schools shall perform risk assessments on the technologies within the school as necessary to ensure that we are fully aware of and can mitigate against the potential risks involved with their use.

Pupils need to know how to cope if they come across inappropriate material or situations online and this will be part of the teaching and learning of E-Safety within each school year.

Whole school risk assessments, as necessary, shall inform the teaching and learning experiences in school to develop best practice in using technologies.

1.4 **Cyber Bullying**

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying, if it takes place within school, will be considered within the schools overall anti-bullying policy, discipline policy and pastoral services provided.

Care should be taken in the future if making use of social media for teaching and learning. Each of the social media technologies can offer much to schools and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation. At present at Beechlawn School we do not use social media to aid teaching and learning and this shall continue until a time when we feel it would be beneficial to our specific pupils and approval is given by the Principal.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.

- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.

- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.

- Mobile Phones (see school Mobile Phone Policy for further information) – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.

- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
  http://www.legislation.gov.uk/nisi/1997/1180

- Malicious Communications (NI) Order 1988
  http://www.legislation.gov.uk/nisi/1988/1849

- The Communications Act 2003
  http://www.legislation.gov.uk/ukpga/2003/21

It is important that pupils are encouraged to report incidents of cyber-bullying to parents first and the school and, if appropriate parents contact the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Schools shall also keep good records of cyber-bullying incidents if they have occurred within school to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

Appendix 1 shows a copy of Cyber Bullying - information for pupils which staff should be familiar with.

1.5 **Communication of the School's E-Safety policy**

The School's E-Safety policy shall be available for all relevant persons including teachers, parents, Governors, support staff and pupils. A copy of the policy shall be provided to all staff and shall be available on learning resources and in the school office.

All staff and pupils shall be made aware that all C2k systems are monitored and that security reports can be accessed by Mrs Green the school principal.

1.6 **Email security**

C2k recommend that all staff and pupils should be encouraged to use their C2k email system. Beechlawn SLT would strongly advise staff not use home email accounts for school business but rather their C2k email accounts.

The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

1.7 **Internet security – The C2K Service**

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password.

Access to the Internet via the C2k Education Network is fully auditable and reports are available to Mrs Green, School Principal and Mr Briggs C2K Coordinator.

Each user will be provided with Internet filtering via the C2k Education Network solution. The new C2k Education Network introduces a revised system for internet filtering based on a Websense filtering solution. Websense assesses all websites based on their content and adds them to a category. Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.

Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.

What's different with the new filtering system?

Previously, we had had access to a number of internet "amber groups" to which users could be added.

The new system categorises all websites as either red (unavailable) or green (available).

By default, all users are given access to a core set of green sites.

School choice:

In addition to the default sites, we can choose to make users members of one or more internet-related security groups. These are:

- Internet_Social Networking
- Internet_Streaming Media
- Internet_Advanced

Access to these groups is controlled by Mr Briggs and Mrs Hanna, who can add individual users or groups of users to these groups via the Identity Management tool in MY-SCHOOL as the educational need arises.

2 **Acceptable Computer Use**

The computer system is owned by the school, and is used by students to access the curriculum, and further their education. The school has drawn up this E Safety and Acceptable Use Policy to protect all parties – the students, the staff and the school. The school reserves the right to examine and delete any files that may be held on the computer system or to monitor any Internet sites visited. This statement serves to fulfil the school's obligations under the Data Protection Act.

- All computer activity should be appropriate to the pupils work, and for their individual education progression. Use for private purposes is not allowed.

- Access must only be made via the authorised account and password.

- Pupils will be held responsible for any inappropriate use of the internet or email provision made through their usernames and passwords.

- The use of the internet and email is externally monitored by the system providers.

- Activity that threatens the integrity of the school ICT Systems or activity that attacks or corrupts other systems is forbidden.

2.1 Rules for pupils use of the Internet

All pupils may be given the opportunity to access the internet in school, as the internet is an excellent teaching tool in the classroom. It is also an excellent learning tool for pupils as it can help them enhance their own independent learning and research skills.

The internet and emailing facilities when provided are for pupils to conduct research and communicate with others and pupils are responsible for good behaviour on the internet just as they are in the classroom.

Pupils should not use the internet to search for or send offensive e-mails, messages or information.

Pupils are to use the internet under the direction of the class teacher.

Appendix 2 shows the Acceptable Use of the Internet Pupil Contract

2.2 Use of Email

- Supervised E-mail may be made available for specific subjects.
- School E-mail facilities must not be used for private correspondence.
- Posting anonymous or offensive messages and forwarding chain letters is strictly forbidden.
- Sending or displaying offensive messages or pictures is forbidden.
- Using obscene language is forbidden
- Harassing, insulting or attacking others is forbidden.

The following are not permitted whilst on the computer:

- Damaging computers, computer systems or computer networks.
- Downloading music.
- Using others' password without permission.
- Trespassing in other pupils' folders, work or files.
- Using IM (Instant Messaging) if not said to do so by the teacher.

Sanctions

Breaking of the rules will result in a temporary or permanent ban of using the internet.

When applicable senior management and parents / guardians will be informed and further consequences may be necessary.

2.3 Multimedia Technology

Introduction

Beechlawn School is aware of the educational benefits the good and proper use of communication technology provides for our pupils, and we do advocate this in order to promote and enhance the learning of our pupils. We are delighted to now have 30 iPads available for pupil use. We however, are also very aware of the potential for personal harm, hurt and damage to individuals by the misuse and abuse of this technology. Consequently the school is therefore concerned with making the provision of multimedia technology safe to use for both pupils and the members of staff who are concerned with using this technology.

Pupil's use of iPads

In school many of the pupils use iPads as an educational tool and this is seen as beneficial by teachers as it helps enhance pupils learning experience;

However pupils are not permitted to use iPads for the following:

- To send inappropriate pictures to others.
- Send hurtful messages.
- Access social networking sites (Facebook, twitter etc) and the Internet without permission.
- Use bad language.
- Send inappropriate photos.
- Take photos of pupils / staff without permission or direction from the teacher.
- Take videos of pupils / staff without permission or direction from the teacher.

Wifi access in school is currently available and Mr Briggs and E Hanna are presently working on the successful and safe introduction of this.

Use of Social networking sites and chat rooms

With the changes C2K are making there is the possibility that pupils will have access to social networking sites in the future, however the school will monitor this and will be dedicated to showing pupils how to

use these sites safely and responsibly when applicable in the curriculum.

However, as pupils have smart phones, tablets, computers etc, they will be able to access such sites from home.

When contacting other pupils on social networking sites pupils should not:

- Use hurtful language.
- Send harmful messages.
- Upload offensive photos.
- Upload personal information about other pupils.

The school is not responsible for pupils' Facebook accounts or other social networking sites and therefore parents are advised to monitor them closely, and ensure that all children's accounts are private.

It is important to note that it is against the law for children under the age of 13 to have a Facebook account.

If a child feels that they are being bullied they should always tell a parent, teacher or another trusted adult.

2.4 Keeping Safe Online

It is important that everyone knows how to keep safe online, below are some guidelines that will help ensure pupils stay safe online.

1. Never share personal details online. For example don't give out your name, address, email or school name.
2. Never give out passwords.
3. Don't believe everything you read or see online.
4. Don't open an e-mail that is suspicious.
5. Tell someone about anything you feel is harmful, hurtful or offensive.
6. Make sure the images you put online are suitable.
7. Respect people's privacy; don't post pictures or videos on the internet without permission.
8. Never speak to strangers or arrange to meet up with them.
9. Always ask a teacher or another trusted person when you are in doubt about something.

2.5 Staff Guidelines on multimedia technology and social networking sites.

This policy is not only aimed at protecting pupils of Beechlawn School but also staff, and therefore staff should follow the guidelines stated below:

Mobile phones and texting

- Most members of staff will not be required to phone or text young people. Consequently they should not have a student's mobile phone number on their phone.
- They should contact students via mobile phone only when necessary. Where possible they should use the school phone to contact pupils.
- Members of staff should **NEVER** respond to informal, social texts from pupils.

Social Networking sites / Chat rooms and Email

- Staff should avoid communicating with students via social networking sites and chat rooms as advised by the school SLT.
- Staff should avoid being "friends" with current pupils in the school on social networking sites.
- Staff should **NEVER** email pupils for social purposes.

2.6 Further staff responsibilities with Internet and Electronic Communications

1. To log on using their provided C2k username and password, this should never be shared with pupils
2. To guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability
3. Ensure that the copying and subsequent use of Internet-derived materials complies with copyright law
4. Not to use personal email accounts during school hours
5. To use C2k supplied email account for professional purposes
6. To ensure written permission from parents or carers has been obtained before images/videos of pupils are electronically published
7. Never to use personal technology to take images or videos of children
8. Carefully select images or videos that include pupils for use in published material
9. Never use pupils' full names anywhere on the website, particularly in association with photographs
10. Not 'befriend' pupils or parents on social networking sites
11. That mobile phones and other devices will be switched off or switched to 'silent' mode. They will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances – they may be used during staff break times but never in view of pupils. Refer to the school mobile phone policy for further information.

12. Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity. Staff will have the use of a school phone where contact with pupils or parents is required.

Further guidance

Users of ICT resources must not engage in any activity that is illegal, distasteful or likely to have negative repercussions for the school. They must not upload, download, use, view, retain, distribute or disseminate in any way any images, video clips, text, attachments, files, materials, software or other similar objects that might be considered indecent, obscene, pornographic, illegal, which might be offensive or that might otherwise be considered inappropriate.

Staff and pupils should note that they are responsible for anything that is done using their user id. They are responsible for all information and data placed on their login, they are also responsible for any e-mails including attachments sent on their login.

All staff are subject to the terms outlined in this policy. Failure to comply may lead to **disciplinary action**.

These guidelines are recommended to keep all staff safe.

Links to other policies

Pastoral Care Policy

Child Protection Policy

Mobile Phone Policy

Discipline Policy

Anti-bullying Policy

Appendix 1 - Cyber Bullying – information for pupils

Cyber bullying means to try to hurt someone's feelings by using technology such as the internet, email, chat rooms, social networking, and applications on multimedia phones such as face time and texting. Cyber bullying can happen to anyone.

If you feel you are being bullied by e-mail, social networking sites, text or online always tell someone you trust.

- Don't reply to bullying, threatening text messages or e-mails this could make things worse.
- Don't give out your personal details online.
- Never share photos of you, friends or family with someone you don't know.
- Never arrange to meet anyone you have met through the internet, social networking sites or through multimedia applications on smart phones.
- Don't send or forward abusive texts or e-mails or images to anyone. Keep abusive messages as evidence.
- Don't ever give out passwords to your mobile or e-mail account.
- Remember that sending abusive or threatening messages is against the law.
- Always tell someone if you feel you are being bullied online or via a smart phone, never keep this to yourself.

If a pupil is identified as engaging in this type of bullying, it will be dealt with by senior management who will impose appropriate sanctions.

Beechlawn School wants to promote a safe environment and therefore Cyber Bullying will not be tolerated.

Appendix 2 <u>Acceptable Use of the Internet Pupil Contract</u>

Beechlawn School provides access for pupils to computers and the internet to help pupils learning and therefore the rules below are employed to help keep everyone safe.

- I will access the computer system with my login and password.
- I will not access other people's files without permission.
- I will only use the school computers for school work and seek direction from the teacher.
- I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
- I will use the Internet responsibly.
- I will only e-mail people I know, or those approved by my teacher using my C2K email account.
- I will not open e-mails sent by someone I don't know.
- The messages I send, or information I upload will be polite and not hurtful to others.
- I will not open attachments, or download a file, unless I have permission from my teacher.
- I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult.
- I understand that the school may check my computer files and may monitor the websites I visit.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

Signed by Pupil: _____

Signed by Parent/ Guardian: _____

Date: _____