E-SAFETY POLICY.

1. Rational
2. Background and purpose
3. Core Principles
4. Aims
5. Dangers of the Internet
6. Use of digital and video images
7. Data protection
8. Bring your own devise
9. Publishing learner's images and work
10. Assessing the risks
11. Measurements taken to prevent the miss use of the internet
12. Roles and responsibilities
13. Education and training

This policy is updated annually and was reviewed February 2018 by Kathryn Black.

1.Rationale

This E-Safety Policy is part of the approach we take to safeguarding the well-being of learners.

This E-Safety Policy has been written by the school, building on government guidance.

2. Background & Purpose

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

1.2 The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

1.3 The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This E- Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all who work, visit and attend the school.

1.4 This policy applies to all members of The Beeches Independent school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

1.5 The Education and Inspections Act 2006 empowers Head of Education, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

1.6 The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of school.

3.Core Principles

The school must comply with a variety of legislation in this regard, including:

i. The Data Protection Act 1998;

ii. The Human Rights Act 1998;

iii. The Computer Misuse Act 1990;

iv. The Regulation of Investigatory Powers Act 2000;

v. The Freedom of information Act 2000;

vi. The Copyright, Designs and Patents Act 1988;

vii. The Electronic Communications Act 2000; together with various Statutory Instruments and other pieces of legislation.

This policy is to be read in conjunction with the school's Behavioural policy, Anti-bullying policy, Safeguarding Policy.

4. Aims

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative, planned e-safety curriculum should be provided as part of IT / PHSE / Life Skills, and any other appropriate lesson, and should be regularly revisited.

• Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.

• Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

• Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

• Students should be helped to understand the need to adopt safe and responsible use both within and outside school.

• Staff should act as good role models in their use of digital technologies the internet and mobile devices.

• In lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

• It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

5. Dangers of the internet.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

5.1

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying, See appendix 1.
- Access to unsuitable video / Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Inappropriate website such as revenge porn websites.

5.2 Many of these risks reflect situations in the off-line world and it is essential that this e- Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

5.3 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

5.4 The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

6. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites. These photographs or videos must not be of any other students or their guest to the school.
- Staff and volunteers are allowed to take digital / video images to support educational aims, 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 taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Student's work can only be published with the permission of the student and parents or carers.

7. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.

• Secure.
• Only transferred to others with adequate protection.

8. Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- Mandatory training is undertaken for all staff.
- Students receive training and guidance on the use of personal devices.
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy.
- Any user leaving the school will follow the process outlined within the BYOD policy.

9. Publishing learner's images and work

Learners' 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 photographs of learners are published on the school website. Learners' work can only be published with the permission of the learner and their parents.

10. Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never

appear on a school computer. The school will not accept liability for the material accessed, or any consequences of Internet access.
The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

11. Measure taken to prevent the misuse of the internet.

- Students are taught 1:1 where possible.
- Students are supervised when using the internet.
- Protection software will be added to all school computers.
- Students will not be allowed at access social media for person use during school times.
- Student's mobile phones and electronic devises will be locked away during school time with other valuables.

12. Roles and Responsibilities

12.1 The following section outlines the roles and responsibilities for e-Safety:

12.2 Head of Education:

• The Head of Education is responsible for ensuring the safety (including e-Safety) of members of the school community.
• The Head of Education / Senior Leaders are responsible for ensuring that staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
• The Head of Education / Senior Management Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
• The Head of Education and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
• Leads on e-Safety.
• Takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents.
• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
• Provides training and advice for staff.
• Liaises with school ICT technical staff.
• Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
• Meets regularly with teaching staff to discuss current issues, review incident logs and filtering / change control logs.
• Reports regularly to Senior Leadership Team.
• That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

• The school's filtering policy is applied and updated on a regular basis.
• That she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant.
• That monitoring software / systems are implemented and updated as agreed in school policies.

12.3 Teaching and Support Staff
are responsible for ensuring that:
• They have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
• They report any suspected misuse or problem to the appropriate person for investigation
• Digital communications with students (e-mail) should be on a professional level and only carried out using official school communication systems
• E-Safety issues are embedded in all aspects of the curriculum and other school activities.
• Students understand and follow the school e-Safety and acceptable use Policy.
• Students have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• They monitor ICT activity in lessons, extra curricular and extended school activities.
• 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.
• In lessons where Internet use is pre-planned students 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.

12.4 Designated senior person for child protection.
Staff should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:
• Sharing of personal data.
• Access to illegal / inappropriate materials.
• Inappropriate on-line contact with adults / strangers.
• Potential or actual incidents of grooming.
• Cyber-bullying.

12.5 Students.
• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
• Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

• Should understand the importance of adopting good e-Safety practice when using digital technologies out of school.

12.6 Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and information about national / local e-Safety campaigns / literature.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and child protection policy.

• The Head of Education (or other nominated person) will receive regular updates through attendance at external training events where appropriate and by reviewing guidance documents released by relevant organisations.

• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

• The head of Education (or other nominated person) will provide advice / guidance / training to individuals as required. *SWGfL BOOST includes an array of presentation resources that the e-Safety coordinator can access to deliver to staff (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources). It includes presenter notes to make it easy to confidently cascade to all staff.*

Appendix 1.What are the different types of cyber bullying?

There are lots of different ways that someone can experience bullying through the internet or mobile phones. Some of them are really subtle, so it might be difficult to realise what is happening.

Text messages
Sending abusive, nasty or threatening text messages to someone is a type of bullying. This could include sharing those texts with other people who might join in the bullying.

Sexting
Sexting is when someone takes a sexually explicit picture or video of themselves and then sends it to someone else. Sometimes people who are trying to bully someone may ask for these kinds of images so they can send them on to other people. If someone's asking you for sexual pictures of yourself, download ChildLine's free Zipit app. It gives you loads of great ways to deal with sexting.

Email
Sending abusive emails is a type of bullying. Sometimes those emails might be shared with other people who could join in the bullying. Sending computer viruses or hurtful videos and pictures by email is also online bullying.

Instant messaging (IM) and chat rooms
Sometimes people might get nasty messages when they are using instant messaging or chat rooms. Sending those types of messages using someone else's account without their permission is also online bullying.

Social networking sites
Social networks can be used in lots of different ways to bully someone. Learn more about how to stop bullying on different social networking sites like Facebook, Twitter, Tumblr, Instagram, YouTube and many more.

Online gaming
Being abusive towards someone or harassing them on an online multi-player gaming site is also a kind of online bullying.

Abusing personal information
Sometimes people involved in bullying might post someone else's photos or personal

information without that person's permission. This could include pretending to be someone else and writing fake comments or blogs.