Beech Hill School

E-safety Policy

Version	**12/18**
Name of Policy Writer	**EducateHR Ltd**
Date Written	**December 2014**
Last Updated	**March 2019**
Next Review Due	**March 2020**

Contents **Page**

1. Introduction

1.1 The aim of this policy is to set out key principles and expectations for all members of the school community with regard to the use of ICT-based technologies. The policy is designed to help safeguard and protect both students and staff in our academy.

1.2 The relevant technologies to which the policy is applicable include, in addition to computers and associated hardware, all electronic devices including (but not limited to) mobile phones, games consoles, cameras and webcams.

1.3 In respect of interaction with students, management will assist staff to work safely and responsibly when utilising the internet and other communication technologies by supporting them in monitoring their own standards and practice.

1.4 There are clear structures in place both to minimise the risk of misplaced or malicious allegations made against staff who work with students and to deal with online abuse such as cyberbullying, sexting (sending and/or receiving personally intimate images) and identity theft including 'frape' (hacking facebook profiles).

1.5 Ofsted describes E-safety (in relation to schools and academies) as the ability to protect and educate students and staff in their use of technology whilst at the same time having appropriate mechanisms in place to intervene and address any incident as and when necessary.

1.6 This policy will be communicated to staff and students (and the wider community as and when appropriate) via school classrooms/staff rooms and website and will be an integral part of the school induction pack for new staff.

1.7 All members of staff in the academy are encouraged (as indeed is the wider community) to exercise vigilance and to be proactive in reporting issues, in the confidence that such concerns will be dealt with quickly and sensitively through the academy's escalation processes.

2. Purpose and scope

2.1 This policy is applicable to all members of our school community who have access to school ICT systems, both on and off school premises. This may include external contractors, trainees, volunteers, parents or carers, visitors, and community users in addition to staff and students.

2.2 The following extract (in relation to cyber-bullying) is taken from the DfE publication 'Preventing and tackling bullying: Advice for headteachers, staff and governing bodies' (July 2017):

> *The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized by a member of staff who has been formally authorised by the headteacher, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.*

2.3 The principle of protecting students includes the provision of a safe learning environment by use of appropriate monitoring and filtering to control what may legitimately be accessed by students whilst at school. Essentially, however, this only protects them whilst they are on

school premises. Ensuring provision of appropriate education relating to E-safety is the only way to guarantee that, irrespective of their whereabouts, they know how to stay safe online.

2.4 The aim of this policy (and indeed of our academy) is both to provide appropriate safeguards and to raise awareness to enable students (and others) to control their online experiences and thereby feel confident and secure in their use of technology. The entire school community needs to be fully aware of the risks (as well as the undoubted benefits) of information technology and accordingly must undertake to use it in a responsible manner.

2.5 Appropriate documents to serve as 'Acceptable Use Policies' (AUPs) and Loan Agreements have been developed which detail the ways in which the internet should be used and such policies (presented in this policy as appendices) are designed be signed by students, their parents/carers, and staff.

2.6 Students will be instructed in the acceptable use of ICT at school, and will be given clear and principled advice and guidance for general use of mobile technologies including the internet. Appropriate objectives are made clear in the student AUPs and are displayed around the school, particularly where internet access is most frequent, such as in computer suites.

2.7 The E-safety policy is integrated (and consistent) with other relevant policies. These include the following: Student Behaviour Policy; (Staff) Disciplinary Policy; Safe Working Practice Policy; Social Media Policy; and Safeguarding Policy.

3. Individual roles and responsibilities

3.1 Headteacher

- To take overall responsibility for the provision of E-safety
- To ensure the school uses an approved, filtered internet service, which is fully compliant with current statutory requirements
- To be responsible for ensuring that staff receive suitable training to carry out their E-safety roles
- To ensure that robust systems are in place to monitor and support staff who carry out internal E-safety procedures (such as school network manager).

3.2 E-safety Co-ordinator (or Designated Safeguarding Lead if applicable)

- To have day to day responsibility for E-safety issues and to perform a leading role in establishing and reviewing the school E-safety policies
- To promote awareness and commitment to E-safeguarding throughout the school community
- To ensure that all staff are aware of procedures that need to be followed in the event of an E-safety incident (including completion of an incident log)
- To regularly update their own knowledge and understanding of E-safety issues and legislation (and to cascade this to other staff) and remain constantly aware of the potential for serious child protection issues
- To liaise with school ICT technical staff
- To liaise with the local authority and relevant agencies as appropriate.

3.3 Governor

- To ensure that the school follows all authoritative E-safety advice to protect the welfare of students and staff
- To approve the E-safety Policy and regularly review the effectiveness of this policy
- To support the school in encouraging parents and the wider community to become engaged in E-safety activities
- To undertake appropriate training and development on E-safety issues.

3.4 Network Manager

- To report promptly to the E-safety coordinator any related issues that may arise
- To ensure that users may only access the school's network through an authorised password reinforced by a robust and properly enforced protection policy
- To ensure that provision exists for both detection of misuse and protection against malicious attack (for instance by keeping virus protection up to date)
- To ensure the overall security of the school ICT system
- To ensure that access controls/encryption are in place to protect all personal and/or sensitive information held on school-owned devices.

3.5 Staff

- To read, understand and help promote the school's E-safety policies and guidance by signing and adhering to the school's 'Staff Acceptable Use Policy' (Appendix 1)
- To be aware of E-safety issues related to the use of mobile phones, cameras and other handheld devices and to monitor their use of such devices to ensure compliance with current school policies
- To report any suspected abuse or breach of policy to the E-safety coordinator
- To maintain an awareness of current E-safety issues, skills development and guidance, for instance through CPD
- To model safe, responsible and professional behaviours in their personal use of information technology.

3.6 Students

- To understand the importance of reporting abuse, misuse or access to inappropriate materials or sites
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To have a good understanding (appropriate to their age and abilities) of research skills and the need to avoid plagiarism and uphold copyright regulations
- *To read, understand, sign and adhere to the Student Acceptable Use Agreement.

3.7 Parents/Carers

- To support the school in promoting E-safety
- To consult with the school if they have any concerns about their children's use of technology
- *To read, understand, sign and adhere (on behalf of their children) to the Student Acceptable Use Agreement.

4. Education, internet and the curriculum

4.1 The academy provides repeated opportunities (within a broad range of curriculum areas) to learn about E-safety and before using the internet students will be made aware of the relevant legislation such as data protection and intellectual property rights.

4.2 Students are also given advice if they experience problems whilst using the internet and/or email and are provided with guidance on promoting E-safety including the requirements to:

- understand the importance of misuse (including accessing inappropriate materials or sites) and are aware of the consequences of this
- understand how to ensure their privacy settings are appropriately configured and to know why they should not post (or share) detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos etc
- understand why they must not post pictures or videos of others without their express consent
- know not to download any files (such as music files) without appropriate permission

4.3 The 'Student Acceptable Use Policy' (Appendix 2) reminds students about their responsibilities and details the strategies to maximise learning opportunities whilst reducing potential risks associated with use of the internet.

5. Managing the ICT infrastructure

5.1 In order to effectively manage internet access (including all relevant security issues) the academy will:

- block all 'chat rooms' and social networking sites other than those which are part of a recognised educational network or approved learning platform
- only unblock (on a strictly time-limited basis) other external social networking sites for specific purposes/internet literacy lessons
- block access to music download or shopping sites other than those approved for recognised educational purposes at a regional or national level
- use security time-outs on internet access where practicable
- ensure all staff and students have signed an acceptable use agreement form
- Inform all users that internet use is open to continuous monitoring
- make clear that in no circumstances is it acceptable for any individual to log on as another user
- set up the network with shared work areas for (separately) students and staff (students and staff are given appropriate instruction in how to save (and subsequently access) work to (or from) these areas)
- require all users to log off at all times when they have either finished working or are leaving the computer unattended (and in the event that a user finds a computer which is logged on but unattended they are required to always log off and then log on again as themselves).
- set up the network so that users cannot download executable files/programmes
- make clear that the academy's IT department is responsible for ensuring that all equipment that is taken off site has full anti-virus and spyware protection and that this is maintained up-to-date in accordance with academy protocols and procedures
- make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the academy is used solely to support their professional responsibilities

6. School website

6.1 The headteacher has overall responsibility for ensuring that the website content is accurate and that the quality of presentation is maintained in full compliance with the statutory DfE guidelines for publications.

6.2 The content of the website will consist primarily of material created by the academy itself. Where the content has been published by others (or there are links to such material) the sources will be credited, with a clear statement as to the author's identity or status.

6.3 Points of contact detailed on the website are likely to include the academy postal address, telephone number and one or more generic email address(es), (such as info@schooladdress or admin@schooladdress). Personal information such as individual e-mail identities will not be disclosed.

6.4 Any photographs published on the web will not have full names attached to them and student names will not be recorded when saving images either in the file names or in the tags when publishing on the academy website.

7. Use of ICT equipment at home

7.1 Staff may be permitted to borrow academy ICT equipment for a time-limited period to pursue core school activities at home. Approval for requests must always be granted before equipment is removed from school premises and the staff member or student must agree and sign the 'Acceptable Use Policy'.

7.2 Staff should be aware that there are only a limited number of such devices and the academy is under no obligation to provide this equipment on demand. If the equipment/computer is used to connect with the internet from the staff member's home, the academy will not be responsible for any costs involved.

8. Use of digital and video photographic images

8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have either recorded themselves or have downloaded from the internet.

8.2 However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may potentially cause significant harm or embarrassment to individuals in the short or longer term.

8.3 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 students should be made aware of the risks attached to publishing their own images on the internet, for instance on social networking sites.

8.4 Images taken and used by the academy will not be kept for longer than is necessary and will be subject to appropriate security measures.

8.5 Staff are allowed to take digital/video images to support educational aims, but must follow academy procedures concerning the sharing, distribution and publication of those images, namely that:

- such images should only be taken on school equipment; the personal equipment of staff should not be used for this purpose
- 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 academy into disrepute
- students must not take, use, share, publish or distribute images of others without their express consent
- photographs published on the website and other publications (such as newsletters etc) which 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 will be obtained from parents/carers (normally in the form of completion of the appropriate AUP) before photographs of students (or examples of their work) are published on the academy website, around school and in school publications.

9. CCTV and monitoring

9.1 The academy has CCTV on the premises as part of site surveillance for staff and student safety. Recordings which are stored for 30 days will not be revealed without permission except where disclosed to the police as part of a criminal investigation.

10. Other policies and procedures

10.1 This policy will be supported by the following policies and procedures:

- Behaviour Policy (student)
- Code of Safe Working Practice
- Disciplinary Policy
- Safeguarding Policy
- Social Media Policy

Appendix 1

Staff Acceptable Use Policy on E-safety

Principles

As an organisation with responsibility for safeguarding of students it is important that all staff take every possible necessary measure to protect data and information systems from unauthorised access, infection, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's information technology equipment in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and related school systems, they are asked to read and sign this Acceptable Use Policy.

Definitions

School Information and Communication Technology

This means any computer, networking device, telephone, copier, printer, fax machine, or other Information and Communication Technology equipment which

- is owned by the school or
- is licensed or leased by the school or
- is subject to school policies.

Roles and responsibilities

<u>The school</u>

The school owns the computers and the internal computer networks used on site. The school also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The school administers, protects, and monitors this aggregation of computers, software, and networks.

In its management of Information and Communication Technology, the school and its administrative department takes responsibility for:

- focusing central Information and Communication Technology resources on activities connected with teaching, learning and administration
- protecting school networks and other shared facilities from malicious or unauthorised use
- ensuring that central school computer systems do not lose important information because of hardware, software, or administrative failures or breakdowns
- managing computing resources so that members of the school community are not denied fair and equitable access to them
- establishing and supporting acceptable standards of security for electronic information that community members produce, use, or distribute, and ensuring the privacy and accuracy of administrative information that the school maintains
- delineating the limits of privacy that can be expected in the use of networked computer resources and preserving freedom of expression over this medium without countenancing abusive or unlawful activities

- monitoring policies and communicating changes in policy as events or technology may warrant
- enforcing policies by restricting access and initiating disciplinary proceedings as appropriate.

The Individual

The school supports networked information resources to further its mission of teaching and learning. All members of the school community must be aware of the rules and conventions that make these resources secure and efficient. Users of school Information and Communication Technology will take responsibility for:

- using resources efficiently, and accepting limitations or restrictions on computing resources - such as storage space, time limits, or amount of resources consumed - when asked to do so by systems administrators
- ensuring that programs from the internet are not downloaded or installed on any school computer: advice should be sought from the ICT Manager as appropriate
- protecting passwords and respecting security restrictions on all systems. If it is believed that a third party is aware of an individual's password the ICT Manager must be notified
- backing up files and other data regularly and permanently removing old files no longer required
- preventing unauthorised network access to or from their computers or computer accounts. This includes the responsible monitoring by staff of student users in their charge
- recognising the limitations to privacy afforded by electronic services
- respecting the rights of others to be free from harassment or intimidation
- honouring copyright, licencing and other intellectual property rights
- ensuring the physical protection of school Information and Communication Technology equipment. Any damage or theft shall be reported to the technical support staff immediately upon detection.
- ensuring responsible use of ICT equipment and ensuring students are following the Acceptable Use Policy
- reporting any faults, problems or requests to the ICT Support Team using the appropriate channels as soon as possible
- Ensuring you are not copying or sharing any personal information belonging to anyone associated with the school unless you have a legal basis for doing so and you are only copying or sharing that data in line with your role within school.
- Ensuring you do not email attachments containing large amounts of personal data (more than three pieces of personal data) unless you encrypt the emails.
- Ensuring home laptops or computers have the requisite network securities and anti-virus software in place if you are using them for work purposes
- Ensuing work on home laptops and computers is saved on encrypted USB sticks.

I understand that it is my responsibility to ensure that I remain up to date and read and understand the school's most recent E-safety policies.

.....

I have read and understood and agree to comply with the Staff Acceptable Use Policy on E-safety and will follow the guidelines in Appendix 1.

Signed: ……..... Print Name: ……

Job Title: ……..... Date: …….....

APPENDIX 1 : Guidelines for Internet and Mobile Telephone Usage for Employees

Introduction
E-mail, the internet and mobile telephones enable staff to have more ready access to information and colleagues. They transform the way we do our jobs and can enrich the working environment.

They are therefore something to be mentioned and used whenever and wherever possible to streamline communication.

The following "traffic light" system has been produced to help staff make effective use of these technologies:

Red (Do not engage in these activities)
- Use e-mail to engage in gossip
- Make libelous statements about individuals or other organisations
- Make statements purporting to represent the school or the council when they are personal views
- Make derogatory remarks or express derogatory opinions about the school or the council
- Knowingly infringe copyright or intellectual property rights
- Knowingly send or receive anything which is illegal or fraudulent
- Knowingly send or receive material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress
- Use the facility to pursue personal business interests, for gambling on for political purposes not directly related to your job.
- Allow anyone else to use your user name and password to gain internet access.
- Knowingly engage in any activity, which threatens the integrity or availability of the school's systems.
- Attempt to break into (HACK) any area.
- Allowing mobile phones to ring during working time

Amber (Seek your manager's approval prior to engaging in the activity)
- Opening and/or sending personal e-mails in working time
- Personal purchases of goods and services via the internet in working time
- Use mobile telephones to receive or make / send personal calls or text messages in work time

Green (Legitimate use)
- Communicate by e-mail or mobile phone on behalf of the school or as an aid to pursuing tasks within the employees job remit
- Conducting research into work related matters
- Personal research of the internet or sending personal e-mails outside working hours
- Personal purchases of goods and services via the internet outside working hours
- Opening personal e-mails outside working time
- Receive/sending personal text messages outside working time
- Receiving/making personal calls outside working time

This list is neither exclusive nor exhaustive if you are in any doubt about where you should be using the facility for a particular purpose – consult a member of the Senior Management Team.

Please note that any failure to comply with the policy may constitute gross misconduct and could lead to disciplinary action. If you inadvertently access a site that contains illegal or offensive material, please inform the ICT manager immediately.

Appendix 2

Student Acceptable Use Policy on E-safety

This Acceptable Use Policy is intended to ensure that young people will be responsible users while using the internet and other communications technologies for educational, personal and recreational use. The school will ensure that ICT systems and users are protected from accidental or deliberate misuse that could place the security of the systems and users at risk.

School strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a staff member
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material
- The school will regularly monitor students' internet usage
- Students and teachers will be provided with training in the area of Internet safety
- Uploading and downloading of non-approved software will not be permitted
- Virus protection software will be used and updated on a regular basis
- The use of personal floppy disks, memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Students will ensure that they log out of their computer equipment when leaving the IT room.

Pupil communication via the Internet

- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person eg cyber-bullying
- Students will not reveal their own or other people's personal details, such as email password, addresses or telephone numbers or pictures
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet
- Students will note that sending and receiving email attachments is subject to permission from their teacher

World Wide Web

- Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials
- Students will report accidental accessing of inappropriate materials in accordance with school procedures
- Students experiencing any issues related to viruses or anti-virus software should inform the ICT Technician without delay
- Students will use the internet for educational purposes only
- Students will not copy information into assignments without express acknowledgement of the source material (plagiarism and copyright infringement)
- Students will never disclose or publicise personal information
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy
- Students will be aware that any usage, including distributing or receiving information whether school-related or personal, may be monitored for unusual activity, security and/or network management reasons

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication that have been accorded prior approval by the school
- Use of chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised
- Usernames will be used to avoid disclosure of identity
- Face-to-face meetings with individuals arranged via internet chat will be expressly forbidden.

Use of digital/video images

The use of digital/video images plays an increasingly important part in learning activities. Students and members of staff may use digital cameras to record evidence of learning and activities. These images may then be used in presentations in subsequent lessons or to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

We will ensure that when such images are published students cannot be identified by the use of their names.

Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

School Website

- Students will be given the opportunity to publish projects, artwork or school work on the world wide web in accordance with clear policies and approval processes regarding the content that may be included in the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of students or staff
- The publication of student work will be co-ordinated by a teacher
- Students' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission. Video clips may be password protected
- Images will not be taken of any student against their wishes
- Photographs taken by our students will be controlled by the school and staff will ensure that they are appropriately supervised in line with the school E-safety policy
- Personal student information including home address and contact details will not be included in school web pages
- The school website will not publish the names of individuals in a photograph.

Personal Devices

Students are not allowed to use their own devices in school for personal use. This will be deemed to be in direct breach of the school's acceptable use policy.

Legislation

The school will provide information on the following legislation relating to use of the internet (with which teachers, students and parents may care to familiarise themselves):

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the internet.

Sanctions

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

I will only use school computers and iPads for my school work.

I will always show respect to the school equipment.

I will always ask an adult to help if there is a problem with any plugs that are connected to the mains electricity.

I will only open and make changes to my own work.

I will never put memory sticks, CDs or other storage devices from home into our school machines.

I will never change passwords or unlock codes of our school's shared devices.

I will only access the internet if my teacher knows.

I will always follow the SMART rules of online safety.

I will minimise my screen and tell my teacher if something makes me uncomfortable online.

I have read and understood, and agree to follow, the school's Acceptable Use Policy on the use of the internet. I undertake to use the internet in a responsible way and to obey all the rules explained to me by the school.

Student's Signature: _____

Name of Student: _____ **Date**: _____