E-safety Policy

Version	**01/24**
Name of Policy Writer	**EducateHR Ltd**
Last Reviewed	**January 2024**
Next Review Due	**January 2025**

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 in relation 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 to minimise the risk of misplaced or malicious allegations made against staff who work with students, and also to deal with internet-related issues such as online abuse (including cyberbullying and sexting – defined as sending and/or receiving personally intimate images) and related topics such as identity theft, including 'frape' (hacking of 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 to be signed, as and when this might be deemed appropriate, by students, their parents/carers, and/or relevant members of 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.

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 (such as school network manager) who carry out internal E-safety procedures.

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's E-safety policy
- 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/Technician

- 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 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
- to read, understand and help promote the school's E-safety policy and related guidance by signing and adhering to the school's 'Staff Acceptable Use Policy' (Appendix 1).

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

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

4. Curriculum

4.1 The academy provides repeated opportunities (within a broad range of curriculum areas) to learn about E-safety. Before accessing the internet for educational purposes 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 be 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
- understand issues around plagiarism and how to check copyright etc
- know not to download any files (such as music files) without appropriate permission
- only use approved class email accounts under supervision by (or with permission from) a teacher.

5. Managing the ICT infrastructure

5.1 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
- 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 level of protection is maintained throughout 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
- ensure that access to the academy's network resources from remote locations by staff is restricted to authorised personnel and that access is only through school approved systems

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 certain email addresses (normally presented in a generic style 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.

6.5 Teachers using academy approved blogs (or similar) will be expected to ensure that these are password protected and to post contributions from the school website only.

7. Use of ICT equipment at home

7.1 In appropriate circumstances 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 must agree and sign the 'Acceptable Use Agreement' (Appendix 1).

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.

7.3 The academy will (as and when resources permit):

- provide a laptop (or other IT equipment) for staff use at home or outside of school
- ensure that the equipment is working and that repairs are dealt with as quickly and effectively as possible
- ensure that the computer is covered by insurance for use in and out of school for study purposes, providing reasonable care is taken to prevent loss or damage
- ensure that the computer is protected against computer viruses and malware
- maintain and update any software used in school.

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. Students should, in particular, 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 permitted 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 never be used for this purpose)
- care should be taken that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute

8.6 In relation to students:

- they must not take, use, share, publish or distribute images of others without their express consent
- photographs taken by students for official school use will be controlled by the academy
- 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
- their 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 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 will not be revealed without permission except where disclosed to the police as part of a criminal investigation.

9.2 Specialist lesson recording equipment may be used on occasion as a tool to share best teaching practice. These recordings are only accessible to authorised members of staff and will not be used for any other purposes.

10. Other policies and procedures

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

- Behaviour Policy (student)
- Code of Conduct and Practice
- Disciplinary Policy

- Safeguarding Policy
- Social Media Policy
- Behaviour 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 (and understanding that 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 (and understanding that any damage or theft is to 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.

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

Signed: ……..... Print Name: ……

Job Title: ……..... Date: …….....

Appendix 2: E-safety Loan Agreement – Staff

Staff may borrow school Information and Technology laptop computers for a time-limited period to pursue core school activities at home. Approval for all requests must be authorised from a member of the senior leadership team prior to equipment being removed from school premises.

Staff are expected to:

- report promptly any loss or damage (including accidental loss or damage)
- report promptly to the IT department any faults in hardware or software
- ensure that the equipment is returned at the end of the agreed time or as soon as the employee ceases to be employed at our school or upon request (whichever is earlier)
- ensure that the equipment is not used for any illegal and/or anti-social purpose, including access to inappropriate internet sites and chat rooms
- ensure that programmes other than those provided by the school are not loaded without prior permission
- take reasonable precautions to prevent the introduction of viruses (and if in any doubt whether a virus may have contaminated the equipment this must be reported before the equipment is connected to the school network)
- ensure that the equipment is transported appropriately and kept securely and protected from damage
- refrain from creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

Failure either to take such reasonable care or to abide by the other conditions listed in this document may result in the computer/equipment being reclaimed. The school also reserves the right to claim financial recompense in such cases (in addition to which disciplinary action may be invoked).

I have read and understand the above and agree to use the school ICT systems and equipment (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

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.

Type of equipment: Laptop (brand) ……. (serial number) …….

Camera ……..... Video camera ……..... Other (specify) …….....

Member of staff signature: …… Job Title: ……

Name …….. Date: ……..

Authorised signatory (SLT) …… Date: ……

Name: …….....