E-Safety Policy

Responsible:	Principal
Responsible Committee:	Teaching and Learning
Review Date	April 2021
Date of Next Review:	June 2023

1. **Aims**

Our Academy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate

2. **Legislation and guidance**

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping ChildrenSafe in Education, and its advice for schools on preventing and tackling bullying and searching, screening andconfiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

3. **Roles and responsibilities**

The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the Principal to account for its implementation. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). The governor who oversees this is Lucy Arnold, safeguarding link.

All governors will

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (appendix 2)

The Principal

The Principal is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.

The Designated Safeguarding Lead (DSL)

Details of the academy's DSL and deputies are set out in our *child protection and safeguarding policy.*

The DSL takes lead responsibilities for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately and in line with the academy's behaviour policy
- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing body

The ICT Manager

The ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online whilst at school, including terrorist and extremist materiel
- Ensuring that the academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the academy's ICT system on a monthly basis (appendix 4)
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported and dealt with appropriately in line with the academy behaviour policy

Passwords

With the advent of increasingly sophisticated password cracking programs, steps need to be taken to minimise the problem posed by malicious users trying to break into accounts. The security of passwords used for accounts held on Global Academy servers is a highly important issue. The passwords used should be carefully considered as badly chosen passwords have the potential to be cracked or easily guessed.

- For staff and students, passwords must be at least seven characters long and should be a combination of letters and numbers
- A password must not be based on anything connected with the individual who owns the account. This includes anything associated with a name or initials, job description, address or postcode.
- Any passwords generated for use by the Global Academy technical support team should be changed immediately after initial use.
- User accounts are issued by the Global Academy technical support team for individual use only
- Accounts and passwords must not be shared, given away or offered for use to anybody else
- Users must take all reasonable steps to keep their passwords confidential and must not disclose them to anyone else
- Passwords should be changed at regular intervals.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the internet (appendix 2), and ensuring that students follow the terms on acceptable use (appendix 1)
- Working with the DSL to ensure that nay online safety incidents are logged (see appendix 3) and dealt with in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately and in line with the behaviour policy

Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Academy's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK safer internet centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet international: http://www.childnet.com/parents-and-carers/hot-topics
- Parent Factsheet, Childnet Interntaional: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- https://www.internetmatters.org

Visitors and members of the community

Visitors and members of the community who use the academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2)

4. **Educating students about online safety**

Students will be taught about online safety as part of the curriculum. Students will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- The safe use of social media and the internet will also be covered within the media curriculum
- The academy will use the PSHE programme to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. **Educating parents about online safety**

The academy will raise parents' awareness of internet safety via our website. This policy will also be shared with parents. Online safety will also be covered during the transition procedure. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. **Cyber-bullying**

Definition

Cyber-bullying takes place on line, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person by another person or group, where the relationship involves an imbalance of power. (See also the academy behaviour policy).

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students as part of safeguarding training (see section 11 for more details)

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the behaviour policy. Where illegal, inappropriate or harmful materiel has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate image or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the complaints procedure.

7. **Acceptable use of the internet in the Academy**

Access to the internet is available for authorised users only. All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1 & 2). Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. All access to the internet at the Global Academy must be via the filtering software installed. This filtering software should help to prevent access to inappropriate sites available over the internet. However, no automatic filter service can be 100% effective in preventing access to such sites and it is possible that users may accidentally access offensive material whilst using the internet. In such circumstance, users must exit the site immediately and advise the person responsible for ICT in the academy, providing details of the site, including the web address, to reduce the possibility of the material being accessed again in the future. The person responsible for ICT will then arrange for the filtering rules to be revised to block the site.

We will monitor the website visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

There is a huge amount of information available to users via the internet, and students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work. Students are not authorised to download software programme onto the academy network.

Acceptable use of the internet is detailed in this E-Safety policy. As a general rule, users should remember that they are acting as a representative of Global Academy and should at all times have regard for legislation when using the internet.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. **Students using mobile devices in the Academy**

Students may bring mobile devices into the academy but are not permitted to use them during

- Lessons, unless directed by the classroom teacher
- Wellbeing
- Tutor group time
- Assemblies
- Lectures/ presentations

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1). Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the academy's behaviour policy, which may result in the confiscation of their device.

Managing personal, student-owned devices (bring your own device) within learning

Students are permitted to use personal electronic devices for educational purposes under the direction of a classroom teacher or teaching assistant. BYOD activities are implemented at the discretion of teachers and technical support team

When electronic devices are used to enhance learning in the classroom, students without a personal device will be provided access to an appropriate academy owned digital device wherever possible.

Violations of any policies, regulations or academy rules involving a student's personal electronic device may result in the loss of use of the device in school and/or disciplinary action. The academy reserves the right to inspect a student's personal electronic device if there is reason to believe that

the student has violated academy policies, regulations, academy rules or has engaged in other misconduct while using their personal electronic device.

The use of an approved personal electronic device is a privilege, and students may be denied access at any time. Students wishing to participate in the Bring Your Own Device program must comply with the following guidelines and procedures.

Social networking sites, Newsgroups and Forums, Chat and Instant Messaging, Personal Websites and Blogs

Conferencing is a powerful method for students and staff to share information and opinions. However, some conferencing applications, including chat and newsgroups sometimes attract undesirable and irrelevant comment. Open access to un-moderated newsgroups by contributors means that newsgroups can be infiltrated by the immature and offensive and for this reason, may not be made available in academies.

As part of the E-Safety sessions run within the curriculum, students will be instructed about access to social networking sites and how such websites will be used within an educational context. Students will be told about the restrictions that apply to personal use and how they should protect their personal information.

Global academy will maintain online systems and Microsoft Office 365, to enable staff, students and parents/ carers to jointly celebrate, share and learn from one another. The tools provided within any online Global academy system and Microsoft Office 365 provide a secure way of introducing students to the world of social networking and how to protect themselves as they become autonomous users of technology systems that fall outside of controlled school environment. These tools include blogs, forum and a video conferencing/ IM solution.

Global academy realises that the majority of young people are using social networking sites. We aim to make students responsible users of these sites and therefore students should be made aware of the advantages and dangers of using these websites.

Media Publications

Video and photographic technologies can be very powerful learning tools. However, photographs and/or video may be taken by staff to support educational aims only. Named images of students will only be published if consent has been given upon enrolment to the academy. Publishing includes, but is not limited to:

- Global Academy & Global websites and social media
- Web broadcasting
- TV presentations
- Newspapers
- Newsletters

Care should be taken when capturing photographs, videos or using video-conferencing to ensure that all students are appropriately dressed and consent has been obtained.

9. **Staff using work devices outside the academy**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the academy's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the academy must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

10. **How the academy will respond to issues of misuse**

Where a student misuses the academy's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. For example, misuse will result in a temporary or permanent ban of internet and/or network.

Where a staff member misuses the academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstance, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. **Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example, through emails, e-bulletins and staff meetings)

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates if applicable

More information about safeguarding training is set out in our Child Protections and Safeguarding Policy.

12. **Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS (appendix 3). An incident log will be part of the governing body safeguarding termly reports. This policy will be reviewed bi-annually by the Vice Principal (behaviour and safety). At every review, the policy will be shared with the governing body.

13. **Links with other policies**

This online safety policy is linked to our:

- Child protection and safeguarding policy

- Behaviour policy
- Staff disciplinary policy
- GDPR, Data protection policy and privacy notices
- Complaints policy

All authorised users will be expected to read, implement and sign to the effect that they know and understand the acceptable use agreement.

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of student:

When using the school's ICT systems and accessing the internet in school, I will not:

- Access or try to access any illegal material;
- Download non-coursework/classwork files/software programmes without permission;
- Use material for classwork / coursework without permission from the copyright holder / owner;
- Actively bypass Global Academy security measures including the use of proxy bypass websitesor VPNs;
- Use or amend images or text that may cause distress or offence;
- Use any ICT equipment to harass, bully, abuse or otherwise distress any individual inside oroutside Global Academy;
- Use Global Academy platform/email to share/distribute files or information that is illegal, ofadult content or may cause offence or distress;
- Without permission, plug in or unplug any computer cables or accessories at any time including the device provided by Global Academy or mobiles phones;
- Log into the network / internet / Microsoft Office 365 and tools, or email with a user name or password that is not your own;
- Use another person's account at any time;
- Store files or download software on your user area that are not related to classwork or coursework;
- Use ICT equipment / Internet for recreational use in Global Academy without permission froma member of staff;
- Access or try to access chat rooms, forums, messaging, social networking or sites with gambling or adult content;
- Use ICT equipment for fraudulent purposes;
- Use images or information on weapons and/ or drugs at any time unless specifically for coursework/classwork;
- Deliberately damage the computer equipment or use the network in a manner that will prevent other using it.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language and/or images when communicating online

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which mightupset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school,and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 1a- Acceptable use of the school's ICT systems and internet and Bring Your Own Device:agreement for pupils and parents/carers

Name of student:

When using the school's ICT systems and accessing the internet in and outside school:

- The Acceptable Use Agreement covers the use of any personal devices with any GlobalAcademy system both inside and outside of an academy site;
- That they are responsible for the safety of their own personal devices, Global Academy is notresponsible for the loss or theft of a device, nor are they responsible for any damage done to the device while at school;
- That they will use their personal device for an educational purpose, and students will only use in class when given permission to do so by the teacher;
- They must keep devices turned off when not using them;
- They may not use the device camera to capture, record, or transmit audio, video or still photos of students, or staff without explicit permission given by the subject of the photo orvideo;
- They must not use the device in a manner that is disruptive to the educational environment inthe academy or allow it to disrupt other users;
- If they misuse their personal device by intimidating behaviour or found bullying through theuse of a personal electronic device.
- They will take precautions to prevent the introduction of computer viruses. If in any doubt whether a virus has contaminated their own personal device, they will report the matterbefore connecting it to Global Academy network.
- If they intend to use their own personal device in school, they will ensure that it is chargedevery evening so that it is ready for use the next day;
- They are responsible for servicing of my personal electronic devices. Global Academy will notservice, repair or maintain any non-Global owned technology brought to, and used at school by staff or students.

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which mightupset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school,and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors,volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a workdevice, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of aviolent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Use any improper language and/or images when communicating online, including in emails orother messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details	
I will only use the school's ICT systems and access the internet in school, or outside school on a workdevice, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected whenusing them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know via CPOMs if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also doso if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my caredo so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety incident report log completed via CPOMs.

https://www.cpoms.co.uk/

Appendix 4: Definitions of Unacceptable Usage

Unacceptable use of computers and network resources may be summarised as:

- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate.
- Threatening, intimidating or harassing employees and students including any message that could constitute bullying or harassment, e.g. on the grounds of gender,race, disability, religion or belief, sexual orientation or age.
- Using obscene, profane or abusive language or images.
- Using language tor images that could be calculated to incite hated against any ethnic, religious or other minority group
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights Defamation (genuine scholarly criticism is permitted)
- Unsolicited advertising often referred to as “spamming”
- Sending emails that purport to come from an individual other than the person actually sending the message using, e.g. a forged address
- Attempts to break into or damage computer systems or data held thereon
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised

- Using the network for unauthenticated access
- Using the ICT facilities to conduct personal commercial business or trading

Restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of policy:

- Downloading, distribution, or storage of music, video, film or other material, for which you do not hold a valid licence or other valid permission form the copyrightholder
- Distribution or storage by any means of pirated software
- Connecting an unauthorised device to the network, i.e. one that has not been configured to comply with this policy and any other relevant regulations andguidelines relating to security, purchasing policy, and acceptable use
- Circumvention of network access control
- Monitoring or interception of network traffic, without permission
- Probing for the security weaknesses of systems by methods such as portscanning, without permission
- Associating any device to network Access Points, including wireless, to which you are not authorised
- Non-academic/non-business related activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services orwhich incur financial costs
- Excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action
- Frivolous use of ICT suites, especially where such activities interfere with others' legitimate use of ICT services
- Copying of other peoples' website material without the express permission of the copyright holder
- Use of peer-to-peer and related applications. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, and KaZaA

Staff and students should consider the spirit of the Global Academy Ethos when working on ICT systems. Any conduct which may discredit or harm the academy, its staff or the ICT facilities or can otherwise be considered intentionally unethical is deemed unacceptable. Incidents of misuse will be dealt with by Global Academy in accordance with the Professional Behaviour (students) or be subject to the disciplinary procedures outlined in the terms and conditions of employment (staff). The appropriate level of sanctions will be applied as determined by the nature of the reported misuse.