E-Safety Policy

Important: This document can only be considered valid when viewed on the Trust website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.	
Name of Responsible Committee:	Standards Committee
Approved Date:	May 2025
Review Date:	May 2026
Target Audience:	Employees, Trustees, pupils, parents
Related Documents: **All Trust policies and procedures referred to are located on the trust website** **If English is not your first language, and you require assistance/translation, please contact the Central Business Services Team**	Behaviour Policy Anti-Bullying Policy Health & Safety Policy Data Protection Policy Safeguarding Policy SEND Policy Exclusion of Pupils Policy

Contents

1. Introduction 3
Scope 3
Roles and Responsibilities 3
2. Why Is Internet Use Important? 3
3. How Does the Internet Benefit Education? 4
4. How Will the Internet Be Used to Enhance Learning? 4
5. How Will Pupils Be Protected? 5
6. How Will Risks Be Assessed? 5
7. How Will Internet/ICT Access Be Authorised? 6
8. E-Mail and Teams Use 6
9. Images On GLA Websites 7
10. Child Sexual Exploitation, Grooming, Cyberbullying and Other Online Dangers 7
11. Managing Emerging Technologies 8
12. Policy Communication 8
13. How will the ICT System Security be Maintained? 10
14. How will Complaints Regarding ICT/Internet use be Handled? 10
15. How Will Parents Support Be Encouraged 10
16. How Do We Monitor the Impact of the E-Safety Policy 11
17. Monitoring and Review 11
Appendix 1 12
Appendix 2: Pupil Acceptable User Agreement 13

1. Introduction

The Internet is an essential element in 21st Century life for education, business and social interaction. Each school has a duty to provide pupils with quality internet access as part of their learning experience.

The Internet and other digital information technologies are powerful tools which open up new prospects for communicating and working with others. Education is embracing these new technologies as they constantly bring with them fresh opportunities for teachers and learners. New skills need to be learnt and applied inside and outside the classroom. At GLA we believe that these new technologies can have a positive impact on the outcomes of our students but we understand that this requires both an understanding of the issues and the teaching of their appropriate and effective use. Fundamentally, e-safety - or online safety - is a safeguarding issue. We recognise that all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse. This policy seeks to explain clearly how this can be done.

Scope

This policy applies to all staff, Trustees, children and parents of the Trust.

Roles and Responsibilities

The **Trust Board** is responsible for approving this policy.

The **CEO** is responsible for ensuring this policy is applied consistently across the Trust.

The **COO** is responsible for the coordination of regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Headteachers.

The **headteachers** are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The **designated safeguarding leads** are responsible for providing reports regarding online safety in school to the headteacher

The **subject leads** are responsible for ensuring staff have a robust understanding of the systems and processes regarding online safety.

The **staff** are responsible for ensuring that they are following this policy and are not in breach of its contents.

2. Why Is Internet Use Important?

The purpose of Internet use in GLA is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management of information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and therefore internet access is an entitlement for pupils who show a sensible approach to its use.

The internet is a tool to enable collaboration between pupils and as a means of engaging with the wider community, including parents/carers.

The internet and IT equipment may be used by visitors to the school, including students, volunteers and helpers.

The internet can support educators in enhancing the offer provided to pupils, through adaptive technology and resources, and can be used to support pupils and enrich learning opportunities.

3. How Does the Internet Benefit Education?

The internet benefits education in the following ways:

- Improved subject learning across a wide range of curriculum areas that promotes excellence and enjoyment, creativity as well as independent learning through cross-curricular project work.
- Access to a wide range of cultural, scientific and intellectual material which might otherwise not be freely or readily available.
- Improved motivation and attitudes to learning.
- Access to online games and activities to support learning.
- Development of problem-solving and research skills.
- Development of network literacy to access resources, create resources and communicate with others
- Access to high quality learning tools
- Access to subscription-based schemes of work and resources to support and develop teaching and learning principles in school
- Access to remote learning resources and communication
- Enhanced social development

4. How Will the Internet Be Used to Enhance Learning?

In GLA schools, pupil internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for internet use.

Pupils will be taught what action to take should they encounter any unsuitable or inappropriate material.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and how to recognise real and false information.

Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Pupils will be taught how to use work collaboratively online, as well as how to save and access their work in an online format, using Microsoft Office 365. Students will be shown how to use these tools safely and responsibly.

5. How Will Pupils Be Protected?

The GLA and its member schools will work in partnership with parents, the LA, DfE, the relevant IT support company and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the head teacher who will inform the Chief Operations Officer via telephone or email and report to the IT support company via the Soft Egg Portal.

Where possible and in conjunction with the IT provider, filtering strategies will be selected to suit the age and curriculum requirements of the pupil, ensuring that restrictions are not unreasonable or restrict what can be taught to children with regards to online teaching and safeguarding.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the member school believes is illegal must be referred to the Internet Watch Foundation, and the Chief Executive informed.
Children will be taught to use and respect the internet and other modern technologies at all times with clear sanctions being in place when either are misused. (see Appendix 1 below)

Pupils will be taught how to be discerning users and recognise signs of false information when online.

Monitoring will suit a primary school setting where staff directly supervise young children whilst using technology. Teachers will consider supervision arrangements including additional support to monitor screen activity during a lesson.

Pupils have individual logins and this can support the monitoring of internet access and activity while in school.

The school will monitor the impact of this policy through logs of reported incidences and through questionnaires and surveys with parents/ carers, pupils and staff.

6. How Will Risks Be Assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. Each member school will take all reasonable precautions to ensure that users access only appropriate material. This includes using an Internet Service Provider which caters specifically for schools. 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 (though it is highly unlikely). Having taken reasonable measures, the school cannot accept liability for the material accessed, or any consequences of Internet access.

Online safety can be broken down into four areas; Conduct (online behaviour), Content (what is available and accessible online), Contact (communication from and to others) and Commercialism (risks such as inappropriate advertising, phishing, online gambling). Children will be taught about these different areas and be educated in how to best deal with any problems.

Methods to identify, assess and minimise risks will be reviewed regularly. In order to reduce risks, the Head Teacher of each member school will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

Parents can at any time inform the school that they do not wish or no longer wish their child to have access to the internet at a member school.

The use of remote learning software will be restricted to allow only required functions, such as the ability to access and return set schoolwork and use certain online software. Direct contact private between pupils, such as email, will be disabled.

7. How Will Internet/ICT Access Be Authorised?

The school will keep a record of all staff and pupils who are granted ICT access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.

Access to approved on-line material via the Internet will be supervised at all times, with age appropriate support/monitoring.
Parents will be asked to read and sign, with their children, a GLA Acceptable Computer and Internet Use Statement (Appendix 1 & 2).

8. E-Mail and Teams Use

Pupils do not currently have personal school email addresses. If these addresses are set up, access will be restricted to ensure emails will only be able to be sent to selected recipients.

Any e-mail sent to an external organisation should be written carefully and checked/authorised by the class teacher before sending.

Pupils must immediately tell a teacher if they receive unpleasant e-mails, if email access is available.

Sanctions will be put in place where it is clear that e-mail is being misused, such as bullying by e-mail. Please refer to anti-bullying policy for the member school policy on bullying.

When TEAMs is used to support learning, it is only utilised for its learning capabilities, such as access to online software (Word, PowerPoint etc) or for children to save evidence of their work.

Pupils have individual access to TEAMs, but in school this access is supervised. Usage can be monitored through Trust administrator accounts.

Messages posted using TEAMs will be polite, respectful and relevant to learning.

Students will be logged out of their Office365 account on the device they have used after each instance where they have been required to use TEAMs/Office365.

9. Images On GLA Websites

Including images of pupils on an school website can be a motivating experience for the pupils of the school and provide the school with opportunities to promote the varied and exciting work that is going on. It is crucial however that careful consideration is taken when deciding how images may be used, and that each member school takes cognisance of the parental permission/s given in regard to use of their child's (children's) images.

The point of contact on the Website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

Written permission from parents or carers will be obtained before photographs of pupils are published on any member school website. The General Data Protection Regulation (GDPR) sets a high standard for consent. As such, our consent forms specify the different ways that photographs are used and parents are asked to consent to each of these. Individuals can say no or withdraw their consent at any time, by contacting the relevant school administrator or the Headteacher. Each school is required to keep a record of consent. Website photographs or the use of digital images that include pupils will be selected carefully. Pupils' full names will not be used anywhere on any website, particularly associated with photographs. If the pupil is named, their photograph will not be used. If a photograph is used, children will not be named with their class or year group being used a general description.

Digital video can also be an exciting medium which can motivate and inspire pupils. We have to make sure that pupils remain unidentifiable if examples of digital video are used on the school website, so reducing the risk of inappropriate contact from outside the school.

Parental permission will be sought before embarking on any digital project. This will apply to all pupils involved in any project, whether they are editing or appearing in the film. Children will not be referred to by name when filming with character names rather than real\names being used where possible. In the credits, the school name will be used as a contact or the class name. Where pupil's names are used in the credits, their first names will only be used. If videos of pupils are used on school websites or within social media, these will not feature names and instead note only class names/year groups.

10. Child Sexual Exploitation, Grooming, Cyberbullying and Other Online Dangers

Pupils will not be allowed or be able to access chat-rooms or Newsgroups under any circumstances in school.

Pupils may be able to use discussion and collaboration tools including a chat facility on carefully monitored platforms as part of the curriculum, e.g. blogging, Teams Channels, jamboards, Padlet

We recognise the dangers of children using devices outside of school and that educating pupils and parents about how to keep safe is part of our duty.

Cyber-bullying: Cyber-bullying takes place online, 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 or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

The DfE has published detailed advice to support schools and colleges to understand child on child sexual violence and sexual harassment (see part 5 of Keeping Children Safe in Education). By helping to prevent cyber-bullying, our schools are also able to help children understand the dangers of exploitation via the internet.

To help prevent cyber-bullying, we will ensure that pupils understand what cyber-bullying is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying in class, and the issue will be addressed in assemblies. This includes personal, social, health (PSHE) education, and other subjects where appropriate. This will also be followed up with information to parents.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

'Stranger danger' is taught to all children in class and through assemblies. GLA schools also make use of outside agencies, e.g. NSPCC, police to make children aware of the dangers online and the way in which exploitation can take place. Children are taught in an age-appropriate way about false identity and predatory behaviour and how to control the settings on the internet to avoid contact with strangers. They are also taught that information is not private and what information is acceptable to share online.

11. Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in member schools is allowed.

12. Policy Communication

Pupils

- The development of a set of 'safe and discriminating behaviours' for pupils to adopt when using the internet and other technologies will be discussed with the children and reinforced. Instruction in responsible and safe use should precede Internet access.
- Children will read, sign and return the 'GLA Acceptable Computer and Internet Use Statement' before access to ICT equipment is given (see appendix 1). Parents will be made aware of this statement and what it covers.
- Rules for Internet access will be posted near all computer and device trolleys or rooms.
- Pupils will be informed that Internet use will be monitored.
- Online safety lessons explicitly teach age appropriate skills which support and reflect this Esafety policy.
- Online safety will also be covered in other subjects, such as RSHE and Computing.
- Additional training will take place, particularly around the issues of social media, 'stranger danger' and Prevent awareness in an age-appropriate manner, the school mindful of issues of cyber-bullying, grooming and sexual exploitation, as well as extremist ideas.

- Older students in Key Stage 2 may be allowed to bring in their own device to school. They will be surrendered to the class teacher/supporting adult on arrival to school and shall be locked away securely and returned to the child at the end of the day.
- Students who bring in their own device must not use the device whilst on school property i.e. the moment they enter the school gates.
- Smart Watches with the capability to send and receive media are not permitted in school and should be surrendered on arrival to school as above.

Sanctions for pupils (please also see Behaviour policy)

- Where misuse has occurred, judgement will be used by the class teacher, Computing Subject Leader, E-safety co-ordinator and member of the Leadership Team or Head Teacher to ascertain whether the misuse was deliberate. Depending upon the seriousness of the offence, internal sanctions will be used. These may range from a first warning or to a temporary withdrawal of Internet privileges. In extreme cases parents or carers will be informed and access to the Internet (and email if applicable) being withdrawn permanently. The behaviour policy of GLA will be referred to when decision are made with regards to sanctions such as 'Red Cards'.
- We reflect 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, our policy 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 pupils' profiles. The Education and Inspections Act 2006 empowers us to such extent as is reasonable, to regulate the behaviour of students 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for, and the deletion of data on electronic devices.
- Any illegal activity will be referred to and dealt with by the police.

Staff and Trustees

- All staff must accept the terms of the 'GLA Acceptable User Agreement' before using any ICT equipment in the school (see GLA Acceptable User Policy).
- All staff including teachers, supply staff, classroom assistants and support staff, and volunteers or visitors working within the school on placement, will be provided with the GLA E-Safety Policy, and its importance explained.
- 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 school's terms of acceptable use, as set out in GLA Acceptable User Agreement.
- 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.
- The GLA does not permit the use of USBs, encrypted or not, and favours the use of school managed, cloud based platforms for saving and sharing documents. Internal sensitive documents must be password protected, with passwords being communicated separately. Any external documents containing sensitive information must be encrypted via LA recommended services (e.g. Egress, Portal).
- If staff have any concerns over the security of their device, they must seek advice from the Chief Operations Officer (COO) or via the Trust's IT support company.
- Work devices must be used solely for work activities.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management. The Designated Safeguarding Lead takes overall responsibility.
- Staff development on safe and responsible Internet use and on GLA E-Safety policy will be provided as required on a regular basis, using the most up to date information available. A particular focus will be given to the connection between internet use (social media) and cyber-bullying, 'stranger danger', Prevent awareness and extremist ideas, grooming and sexual exploitation. Staff will be trained on how to support, guide and teach children in an age-appropriate way, whilst able to recognise the signs of exploitation or abuse.
- Trustees will receive training on the above issues as required and will be required to monitor e-safety as part of their responsibility for safeguarding.
- If, at any point, there is a risk of immediate serious harm to a child a referral should be made to the designated safeguarding lead with reference to the safeguarding policy
- Any communication sent via email regarding pupils should make use of the registered domain name for each school e.g. bishopscleeve.gloucs.sch.uk or from the overall Trust domain e.g. glatrust.org.uk
- Should a member of staff have concerns over the conduct of a colleague or adult working at GLA, they must adhere to GLA Whistleblowing Policy.

13. How will the ICT System Security be Maintained?

Soft Egg are employed by each school to ensure the following:

- The school ICT systems will be reviewed regularly with regard to security. Virus protection will be installed and updated regularly.
- Files held on the school's network will be regularly checked.
- That the system has the capacity to take increased traffic caused by Internet use.

14. How will Complaints Regarding ICT/Internet use be Handled?

Any complaint about staff misuse must be referred to the Head Teacher and will then be pursued through the GLA disciplinary procedures as appropriate.

Pupils and parents will be advised that any complaints regarding internet use should be pursued through the GLA complaints procedure and pursued as appropriate.

15. How Will Parents Support Be Encouraged

Parents' attention will be drawn to the school E-Safety Policy in newsletters and on member school websites.

Children will read, sign and return the 'GLA Acceptable Computer and Internet Use Statement' prior to using school ICT equipment (see appendix 1). Parents will be able to access this.

A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be developed and made available to parents. Information on e-safety can be found at https://www.commonsensemedia.org/, https://www.thinkuknow.co.uk/,

https://www.nspcc.org.uk/keeping-children-safe/online-safety/ and https://saferinternet.org.uk/

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to student records through Learning Platform such as Arbor.
- Their children's personal devices in the school.

Specific and up to date advice and guidance will be provided to parents regularly through various communication mediums including website, social media, newsletters and information events specifically relating to the growth of social media and the connection of internet use and exploitation, particularly around the issues of cyber-bullying, grooming and sexual exploitation as well extremist ideas and Prevent awareness.

16. How Do We Monitor the Impact of the E-Safety Policy

The policy and provision is evaluated through an annual audit, each school using their own toolkit of resources which may include SWGfL 360 audit tool

The reported incidences are recorded and number of incidences reported, each school using their own secure online systems such as CPOMS

Pupil and parent surveys

17. Monitoring and Review

E-Safety is an area that is constantly evolving and as such this policy will be reviewed annually or in response to an E-Safety incident, whichever is sooner. The policy will be reviewed by the Chief Executive and ratified by the Trust Board.

Appendix 1

Guidelines For Acceptable Computer & Internet Use

The Academies within the GLA and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

Unmonitored social networking is not supported in our Academies and we recommend parents carefully monitor how children interact online and consider the age recommendations for usage .

Parents should promote and model good online citizenship, ensuring that any messages or posts relating to the Academy are polite and in the spirit of celebration.

SuperCATs will…

- **Check** with an adult before they use any programmes, download anything or click anything they don't understand
- **Ask** an adult before they go online or use IT equipment, or if they need help using the IT equipment, programmes, games or websites.
- **Tell** an adult if they see something that worries, upsets or scares them when they're online
- Use IT equipment sensibly, including using sensible search terms online
- Look after the equipment and tell an adult if something is broken
- Keep personal details and passwords safe
- Be kind online! When communicating, use nice words and be respectful

While in school, my computer use will be monitored. If I break these rules, I might not be allowed to use computers or the internet.

Appendix 2: Pupil Acceptable User Agreement

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.
- I will surrender any device, including Smart Watches, when I arrive at school so a teacher/adult can store it safely until the end of the day: use of personal devices on school grounds is strictly forbidden.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that

others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will not download anything without asking a trusted adult first (teacher or parent)
- I will only use sensible and appropriate search terms when carrying out searches online.
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to negative consequences. This could include loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Class: .....

Signed: ..... Date: .....